CA Enterprise Log Manager

Notes de parution

r12.1 SP3



Produits CA référencés

Ce document fait référence aux produits CA suivants :

- CA Access Control
- CA Audit
- CA ACF2™
- CA Directory
- CA Embedded Entitlements Manager (CA EEM)
- CA Enterprise Log Manager
- CA Identity Manager
- CA IT Process Automation Manager (CA IT PAM)
- CA NSM
- CA Security Command Center (CA SCC)
- Poste de service CA
- CA SiteMinder®
- CA Spectrum®
- CA Top Secret®

Support technique

Pour une assistance technique en ligne et une liste complète des sites, horaires d'ouverture et numéros de téléphone, contactez le support technique à l'adresse http://www.ca.com/worldwide.

Modifications de la documentation

Les mises à jour suivantes ont été réalisées depuis la dernière version de la présente documentation.

- Fonctionnalités ajoutées et modifiées dans la version 12.1 SP3 : Ce chapitre contient les informations relatives à la nouvelle fonctionnalité incluse dans cette version.
- Les problèmes connus suivants ont été supprimés, étant donné qu'ils ont été réglés et ne s'appliquent plus à cette mise à jour :
  - Impact du nom d'application personnalisé sur une requête d'archive

Informations complémentaires :

Mise à niveau par abonnement (page 11)
Fonctionnalités r12.1 SP1 ajoutées et modifiées (page 37)
Conformité à la norme FIPS 140-2 (page 37)
Modes de fonctionnement (page 38)
Bibliothèques de chiffrement (page 39)
Algorithmes utilisés (page 39)
Certificats et fichiers clés (page 40)
Limitations de la prise en charge de la norme FIPS (page 42)
Configuration de Microsoft Internet Explorer pour l'accès à CA Enterprise Log Manager en mode FIPS (page 43)
Configuration de Mozilla Firefox pour l'accès à CA Enterprise Log Manager en mode FIPS (page 44)

Table des matières

Chapitre 7 : Fonctionnalités r12.1 ajoutées et modifiées 47

Chapitre 8 : Problèmes connus 51

Chapitre 1 : Bienvenue

Bienvenue dans CA Enterprise Log Manager Ce document contient des informations relatives aux systèmes d'exploitation pris en charge, aux améliorations, aux problèmes connus et au support technique de CA.

Mise à niveau par abonnement

Vous pouvez mettre CA Enterprise Log Manager à niveau vers la version ou vers le Service Pack les plus récents en téléchargeant tous les modules livrés par abonnement.

Important : Vous devez mettre à niveau le serveur CA Enterprise Log Manager de gestion avant d'installer des nouveaux serveurs CA Enterprise Log Manager dans votre réseau. Cela garantit l'enregistrement des nouveaux serveurs.

Procédez comme suit.

1. Vérifiez la configuration de base de l'abonnement.
   a. Cliquez sur l'onglet Administration, sur le sous-onglet Services, puis sélectionnez Module d'abonnement.
   b. Sélectionnez non pour Redémarrage automatique après mise à jour du SE.
   c. Déplacez le module Gestionnaire de journaux vers la liste des éléments sélectionnés, si elle ne s'y trouve pas déjà.
   d. Vérifiez que toutes les valeurs requises sont configurées au niveau global.
   e. Vérifiez que toutes les valeurs requises sont configurées pour chaque serveur CA Enterprise Log Manager.

   Remarque : Dans des environnements fédérés, mettez à jour les parents avant les enfants.

   Un événement d'autosurveillance déclarant que les mises à jour d'abonnement ont été installées indique la fin.

2. Vérifiez la configuration de base de l'abonnement.
   a. Cliquez sur l'onglet Administration, sur le sous-onglet Services, puis sélectionnez Module d'abonnement.
   b. Sélectionnez non pour Redémarrage automatique après mise à jour du SE.
   c. Déplacez vers la liste des éléments sélectionnés tous les modules à télécharger.

   Remarque : Dans des environnements fédérés, mettez à jour les parents avant les enfants.
3. Lorsque le processus de mise à jour d'abonnement est terminé, redémarrez chaque serveur CA Enterprise Log Manager.

   Un événement d'autosurveillance déclarant que les mises à jour d'abonnement ont été installées indique la fin.
4. Mettez à jour les agents et les connecteurs comme suit.
   a. Cliquez sur l'onglet Administration, sur le sous-onglet Collecte de journaux, puis sélectionnez Explorateur d'agent.
   b. Déterminez si les mises à jour d'abonnement doivent être appliquées au niveau de l'Explorateur d'agent, des groupes d'agents ou des agents.
   c. Sélectionnez le niveau souhaité, puis cliquez sur le bouton Abonnement.
   d. Appliquez les mises à jour aux agents si Agents faisait partie des modules téléchargés.
   e. Cliquez à nouveau sur le bouton Abonnement.
   f. Appliquez les mises à jour aux connecteurs, si disponibles.
5. Réenregistrez les produits tiers et les autres produits CA (CA Access Control par exemple) utilisant des appels d'API ouverte pour afficher des rapports CA Enterprise Log Manager dans leur interface native.

   Cette étape met à jour les certificats modifiés dans cette version. Pour de plus amples informations, consultez le *Manuel de programmation de l'API CA Enterprise Log Manager*.

Remarque : Pour connaître les problèmes connus liés à la mise à niveau d'un abonnement, reportez-vous aux notes de parution.

Informations complémentaires :

Redémarrage automatique après mise à jour du SE lors d'une mise à niveau de SP (page 61)

Chapitre 2 : Environnement d'exploitation

Ce chapitre traite des sujets suivants :

Environnements matériel et logiciel

Lors de son installation initiale, CA Enterprise Log Manager installe également le système d'exploitation Red Hat Enterprise Linux.

L'index de la matrice de certification CA Enterprise Log Manager inclut les liens vers les matrices de certification CA Enterprise Log Manager, dont les liens suivants :

- Matériel et logiciels de serveur

  Matrice de certification du matériel et des logiciels du serveur CA Enterprise Log Manager

- Matériel et logiciels d'agent

  Matrice de certification du matériel et des logiciels de l'agent CA Enterprise Log Manager

- Prise en charge des détecteurs de journal et des systèmes d'exploitation connexes

  Matrice de certification du détecteur de journal CA Enterprise Log Manager

- Intégrations du produit

  Matrice d'intégration du produit CA Enterprise Log Manager

- Certifications avec CA Audit iRecorder

  Matrice de certification CA Enterprise Log Manager Audit iRecorder

Vous pouvez accéder à CA Enterprise Log Manager au moyen des navigateurs suivants, ainsi qu'avec Adobe Flash Player 9 ou 10.

- Internet Explorer 6 SP2 (uniquement en mode non FIPS)
- Internet Explorer 7 ou 8 (modes FIPS ou non FIPS)
- Mozilla Firefox 2.0.x et 3.0.x (uniquement en mode non FIPS)
- Mozilla Firefox 3.5.8 ou version ultérieure (modes FIPS et non FIPS)

Remarque : Les exportations de fichiers ne fonctionnent pas lorsque vous accédez à CA Enterprise Log Manager avec un navigateur Mozilla Firefox.

Conditions préalables à la configuration avancée pour certains ordinateurs HP et IBM

Lorsque CA Enterprise Log Manager est installé sur des serveurs HP Proliant DL 380G5 Series et IBM X3650 Series avec les paramètres par défaut d'utilisation de l'alimentation, des problèmes peuvent survenir au niveau d'iGateway et ralentir le fonctionnement, ou encore, au niveau de l'interface et requérir le redémarrage manuel du service.

Pour empêcher que cela ne soit le cas, modifiez les paramètres avant d'installer CA Enterprise Log Manager.

Remarque : Si vous avez déjà installé CA Enterprise Log Manager, vous pouvez éteindre l'ordinateur, modifier les paramètres comme indiqué et redémarrer l'ordinateur.

Pour modifier les paramètres d'utilisation de l'alimentation sur un serveur HP Proliant DL 380G5 :

1. Accédez au menu BIOS Settings (paramètres du BIOS).
2. Naviguez jusqu'aux paramètres d'utilisation de l'alimentation.
3. Sélectionnez OS Control Mode.

   Remarque : Le paramètre par défaut est HP Dynamic Power Settings Mode.

Pour modifier les paramètres d'utilisation de l'alimentation sur un serveur IBM X3650 :

1. Accédez au menu BIOS Settings (paramètres du BIOS).
2. Naviguez jusqu'aux paramètres d'utilisation de l'alimentation.
3. Désactivez les paramètres suivants.
   - Active Energy Manager
   - Enhanced C1 Power State

Résolution de l'écran

La résolution d'écran minimale requise est de 1024 x 768 pixels. Pour un affichage plus confortable, la résolution de 1280 x 1024 est recommandée.

Références du serveur CA EEM

Pour obtenir des informations sur la prise en charge des systèmes d'exploitation par un serveur CA EEM existant, consultez le manuel de *mise en oeuvre de CA Embedded Entitlements Manager*. Ce manuel fait partie de la bibliothèque CA Enterprise Log Manager.

Vous pouvez également télécharger cette bibliothèque à partir du support technique. En cas de problème, n'hésitez pas à contacter notre service d'assistance technique à l'adresse http://www.ca.com/worldwide.

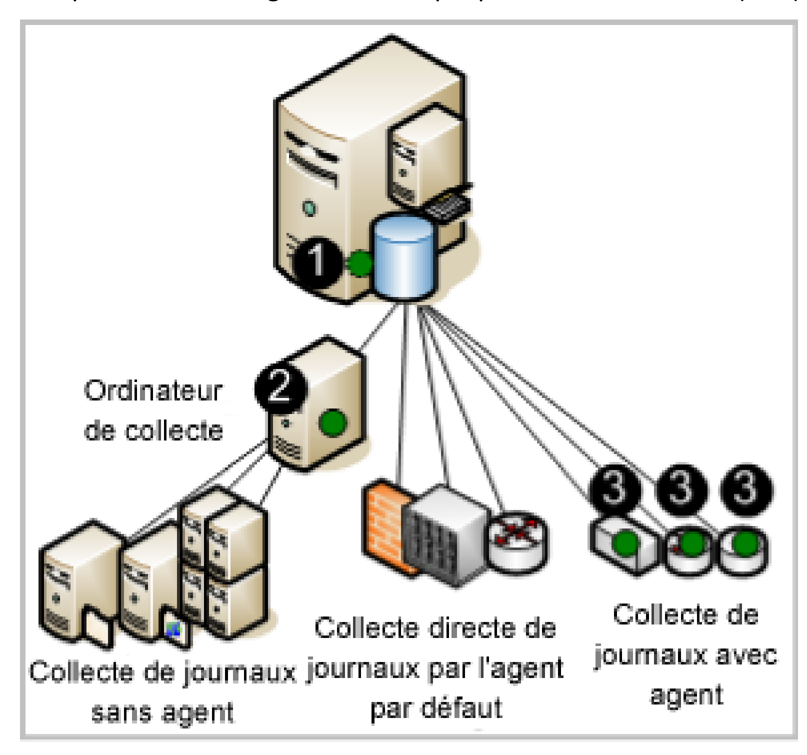
Chapitre 3 : Fonctionnalités

Ce chapitre traite des sujets suivants :

Collecte de journaux

Le serveur CA Enterprise Log Manager peut être configuré pour collecter des journaux à l'aide d'une ou de plusieurs techniques prises en charge. Les techniques diffèrent quant au type et à l'emplacement du composant qui écoute et collecte les journaux. Ces composants sont configurés sur les agents.

L'illustration ci-dessous décrit un système avec un seul serveur, où l'emplacement des agents est indiqué par un cercle sombre (vert).



Les numéros sur l'illustration se rapportent aux étapes ci-dessous.

1. Configurez l'agent par défaut sur CA Enterprise Log Manager pour récupérer directement des événements auprès des sources Syslog spécifiées.
2. Configurez l'agent installé sur un point de collecte Windows pour collecter des événements provenant des serveurs Windows spécifiés et les transmettre à CA Enterprise Log Manager.
3. Configurez les agents installés sur des hôtes où sont exécutées les sources d'événement, pour collecter le type d'événement configuré et effectuer la suppression.

Remarque : Le trafic entre l'agent et le serveur CA Enterprise Log Manager de destination est toujours chiffré.

Etudiez les avantages de chaque technique de collecte de journaux ci-dessous.

- Collecte directe de journaux

  Avec la collecte directe de journaux, vous configurez l'écouteur Syslog sur l'agent par défaut pour recevoir les événements des sources fiables spécifiées. Vous pouvez également configurer d'autres connecteurs pour collecter des événements provenant de n'importe quelle source d'événement compatible avec l'environnement de fonctionnement du dispositif logiciel.

  Avantage : vous n'avez pas besoin d'installer un agent pour collecter les journaux des sources d'événement à proximité du serveur CA Enterprise Log Manager sur le réseau.

- Collecte sans agent

  Avec la collecte sans agent, il n'existe aucun agent local sur les sources d'événement. Au lieu de cela, un agent est installé sur un point de collecte dédié. Des connecteurs sont configurés pour chaque source d'événement cible sur cet agent.

  Avantage : vous pouvez collecter des journaux provenant de sources d'événement s'exécutant sur des serveurs où vous ne pouvez pas installer d'agents, comme des serveurs où la stratégie d'entreprise interdit les agents. La remise est garantie, par exemple, lorsque la collecte de journaux ODBC est correctement configurée.

- Collecte avec agent

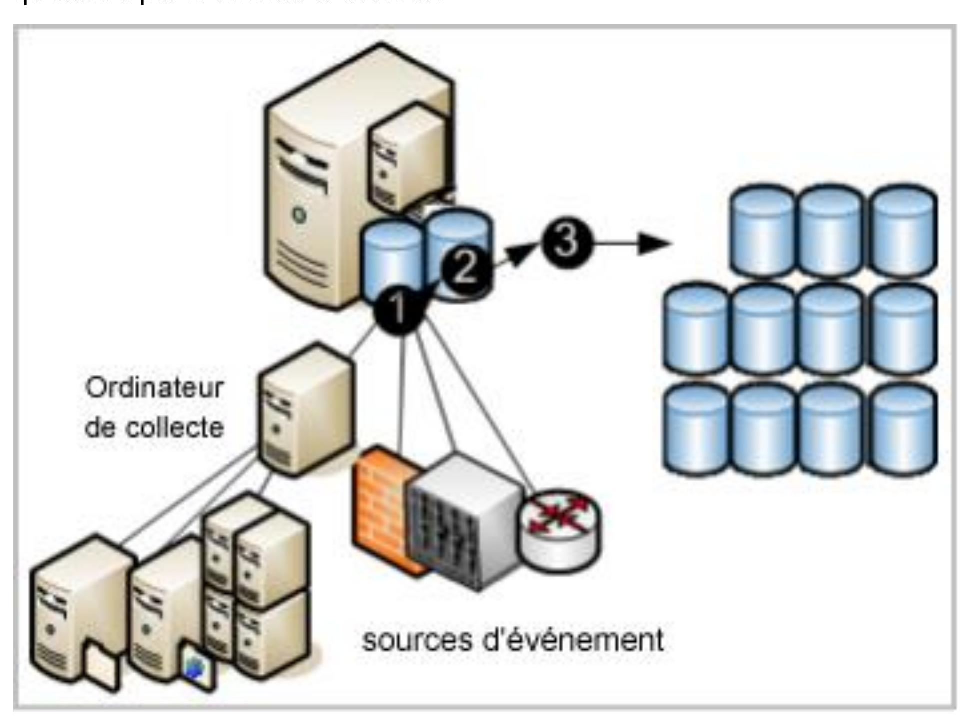
  Pour la collecte avec agent, un agent est installé lorsqu'une ou plusieurs sources d'événement sont exécutées et qu'un connecteur est configuré pour chaque source d'événement.

  Avantage : vous pouvez collecter des journaux provenant d'une source pour laquelle la bande passante du réseau vers CA Enterprise Log Manager n'est pas suffisamment efficace pour prendre en charge la collecte directe de journaux. Vous pouvez utiliser l'agent pour filtrer les événements et réduire le trafic émis sur le réseau. La remise d'événement est garantie.

Remarque : Pour plus de détails sur la configuration des agents, consultez le *Manuel d'administration*.

Stockage des journaux

CA Enterprise Log Manager dispose du stockage intégré et géré des journaux des bases de données récemment archivées. Les événements collectés par les agents provenant de sources d'événement suivent un cycle de stockage tel qu'illustré par le schéma ci-dessous.



Les numéros sur l'illustration se rapportent aux étapes ci-dessous.

1. Les nouveaux événements collectés par n'importe quelle technique sont envoyés à CA Enterprise Log Manager. L'état des événements entrants dépend de la technique utilisée pour les collecter. Les événements entrants doivent être ajustés avant d'être insérés dans la base de données.
2. Lorsque la base de données des enregistrements ajustés atteint la taille configurée, tous les enregistrements sont compressés en une base de données et enregistrés sous un seul nom. La compression des données des journaux réduit les coûts induits par leur déplacement et leur stockage. La base de données compressée peut être déplacée automatiquement en fonction de la configuration de l'archivage automatique ; vous pouvez également la sauvegarder et la déplacer manuellement avant qu'elle n'atteigne la durée configurée avant suppression (les bases de données archivées automatiquement sont supprimées de la source dès qu'elles sont déplacées).
3. Si vous configurez l'archivage automatique pour qu'il déplace chaque jour les bases de données compressées vers un serveur distant, vous pouvez déplacer ces sauvegardes vers un stockage de journaux hors site à long terme si vous le souhaitez. En conservant les sauvegardes des journaux, vous respectez les réglementations stipulant que les journaux doivent être collectés de manière sécurisée, stockés de manière centralisée pendant un certain nombre d'années et disponibles pour être examinés (vous pouvez restaurer la base de données à tout moment depuis le stockage à long terme).

Remarque : Pour plus de détails sur la configuration du magasin de journaux d'événements, y compris la configuration de l'archivage automatique, consultez le *Manuel d'implémentation*. Pour plus de détails sur la restauration des sauvegardes à des fins d'examen et de génération de rapports, consultez le *Manuel d'administration*.

Présentation normalisée des journaux

Les journaux générés par les applications, les systèmes d'exploitation et les unités utilisent tous leur propre format. CA Enterprise Log Manager ajuste les journaux collectés afin de normaliser la consignation des données. Le format standard facilite la comparaison des données collectées auprès de différentes sources pour les auditeurs et les cadres supérieurs. Techniquement, le CEG (Common Event Grammar) CA facilite l'implémentation de la normalisation et de la classification des événements.

La CEG propose plusieurs champs utilisés pour normaliser différents aspects de l'événement, notamment ceux répertoriés ci-dessous.

- Modèle idéal (classe de technologies comme les antivirus, les SGBD et les pare-feu)
- Catégorie (par exemple Gestion des identités et Sécurité du réseau)
- Classe (par exemple Gestion des comptes et Gestion de groupes)
- Action (par exemple Création d'un compte et Création d'un groupe)
- Résultats (par exemple Opération réussie et Echec)

Remarque : Pour plus de détails sur les règles et fichiers utilisés lors de l'ajustement des événements, consultez le *Manuel d'administration CA Enterprise Log Manager*. Consultez la section relative à la Grammaire commune aux événements dans l'aide en ligne pour de plus amples détails sur la normalisation et la classification des événements.

Génération de rapports de conformité

CA Enterprise Log Manager vous permet de collecter et de traiter des données relatives à la sécurité, puis de les transformer en rapports appropriés pour les auditeurs internes ou externes. Vous pouvez interagir par le biais de requêtes et de rapports à des fins d'examen. Vous pouvez automatiser le processus de génération de rapports en planifiant les jobs de rapport.

Le système offre les avantages ci-dessous.

- Simplicité de formulation de requêtes, grâce aux balises
- Génération de rapports en temps quasi-réel
- Centralisation de la recherche dans les archives distribuées des journaux critiques

Il se concentre sur la génération de rapports de conformité plutôt que sur la corrélation en temps réel des événements et alertes. La réglementation exige la génération de rapports prouvant la conformité avec les contrôles relatifs au secteur. CA Enterprise Log Manager fournit des rapports contenant les balises ci-dessous pour faciliter l'identification.

- Basel II
- COBIT
- COSO
- Directive UE - Protection des données
- FISMA
- GLBA
- HIPAA
- ISO\IEC 27001\2
- JPIPA
- JSOX
- NERC
- NISPOM
- PCI
- SAS 70
- SOX

Vous pouvez examiner des rapports de journaux prédéfinis ou effectuer des recherches en fonction de critères spécifiés par vos soins. De nouveaux rapports sont fournis avec les mises à jour d'abonnement.

Les fonctionnalités d'affichage des journaux reposent sur les éléments suivants :

- Requêtes à la demande, prédéfinies ou définies par l'utilisateur, dont les résultats peuvent atteindre jusqu'à 5 000 enregistrements
- Recherche rapide, au moyen d'invites, pour un nom d'hôte, une adresse IP, un numéro de port ou un nom d'utilisateur spécifié
- Génération de rapports planifiée et à la demande, avec contenu de génération de rapports prêt à l'emploi
- Requêtes et alertes planifiées
- Rapports de base avec informations de tendances
- Visionneuses d'événements interactives et graphiques
- Génération automatisée de rapport avec pièce jointe de courriel
- Stratégies de conservation automatisée de rapport

Remarque : Pour plus de détails sur l'utilisation de requêtes et de rapports prédéfinis ou sur la création de requêtes et de rapports personnalisés, consultez le *Manuel d'administration CA Enterprise Log Manager*.

Alerte de violation de stratégie

CA Enterprise Log Manager vous permet d'automatiser l'envoi d'un courriel d'alerte lorsque survient un événement qui nécessite une attention à court terme. Vous pouvez également surveiller à tout instant les alertes d'action à partir de CA Enterprise Log Manager, en spécifiant un intervalle de temps, depuis les cinq dernières minutes jusqu'aux 30 derniers jours écoulés. Des alertes sont envoyées automatiquement à un flux RSS auquel il est possible d'accéder à partir d'un navigateur Web. Si vous le souhaitez, vous pouvez spécifier d'autres destinations, y compris des adresses électroniques, un processus CA IT PAM, qui génère des tickets de bureau d'assistance, et une ou plusieurs adresses IP de destination d'interruption SNMP.

Pour vous aider à commencer, de nombreuses requêtes prédéfinies sont disponibles pour être planifiées, sans modification, en alertes d'action. Quelques exemples sont présentés ci-dessous.

- Activité excessive de l'utilisateur
- Utilisation élevée de l'UC
- Peu d'espace disque disponible
- Journal des événements de sécurité effacé au cours des dernières 24 heures
- Stratégie d'audit Windows modifiée au cours des dernières 24 heures

Certaines requêtes comportent des listes à clés, où vous fournissez les valeurs utilisées par la requête. Certaines listes à clés contiennent des valeurs prédéfinies que vous pouvez compléter, par exemple les comptes par défaut et les groupes avec droits. D'autres listes à clés, comme celle des ressources stratégiques, ne comportent pas de valeurs par défaut. Une fois configurées, des alertes peuvent être planifiées pour des requêtes prédéfinies comme celles répertoriées ci-dessous.

- Ajout ou retrait d'une appartenance à un groupe par des groupes avec droits.
- Connexion établie par le compte par défaut
- Aucun événement reçu par les sources stratégiques.

Les listes à clés peuvent être mises à jour manuellement, en important un fichier, ou en exécutant un traitement des valeurs dynamiques de CA IT PAM.

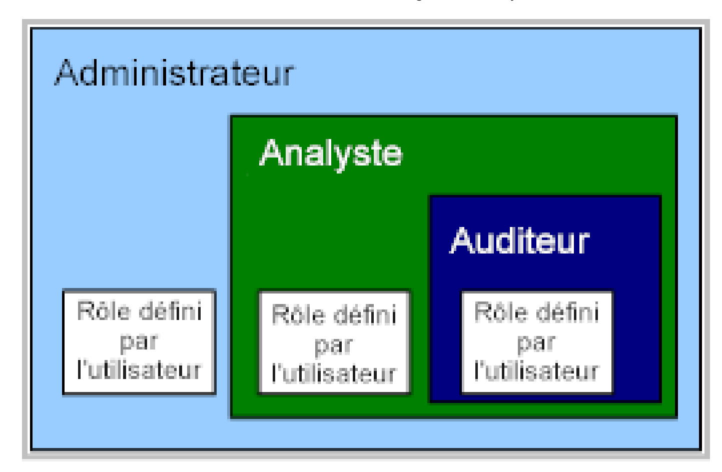
Remarque : Pour plus de détails sur les alertes d'action, consultez le *Manuel d'administration CA Enterprise Log Manager*.

Accès selon un rôle

CA Enterprise Log Manager propose trois groupes d'applications ou rôles prédéfinis. Les administrateurs affectent les rôles ci-dessous aux utilisateurs, pour spécifier leurs droits d'accès aux fonctions CA Enterprise Log Manager.

- Administrator
- Analyst
- Auditor

L'auditeur peut accéder à quelques fonctions. L'analyste peut accéder à toutes les fonctions Auditor, auxquelles s'ajoutent quelques autres fonctions. L'administrateur peut accéder à toutes les fonctions. Vous pouvez définir un rôle personnalisé avec des stratégies associées qui limitent l'accès de l'utilisateur aux ressources, de façon à répondre à vos besoins commerciaux.



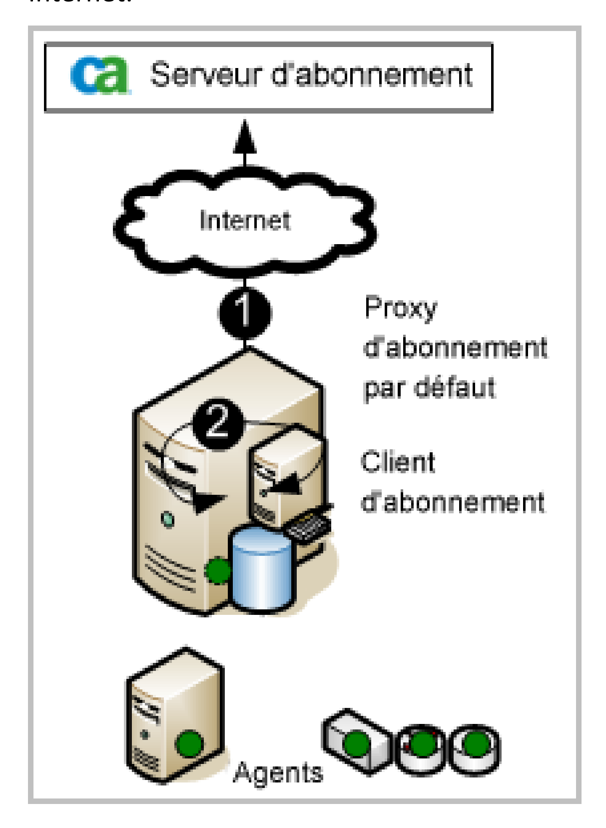
Les administrateurs peuvent personnaliser l'accès à n'importe quelle ressource en créant un groupe d'applications personnalisé avec des stratégies associées, puis en affectant ce groupe d'applications, ou rôle, aux comptes d'utilisateur.

Remarque : Pour plus de détails sur la planification et la création de rôles personnalisés, de stratégies personnalisées et de filtres d'accès, consultez le *Manuel d'administration CA Enterprise Log Manager*.

Gestion de l'abonnement

Le module d'abonnement est le service qui permet de télécharger automatiquement, de manière planifiée, les mises à jour d'abonnement provenant du serveur d'abonnement CA et de les distribuer aux serveurs CA Enterprise Log Manager. Lorsqu'une mise à jour d'abonnement inclut le module pour les agents, les utilisateurs lancent le déploiement de ces mises à jour vers les agents. *Les mises à jour d'abonnement* sont des mises à jour de composants CA Enterprise Log Manager, ainsi que des mises à jour de système d'exploitation, des correctifs et des mises à jour de contenu, comme les rapports.

L'illustration ci-dessous décrit le scénario le plus simple de connexion directe à Internet.



Les numéros sur l'illustration se rapportent aux étapes ci-dessous.

1. Le serveur CA Enterprise Log Manager, en tant que serveur d'abonnements par défaut, contacte le serveur d'abonnements CA concernant les mises à jour et télécharge toute mise à jour nouvellement disponible. Le serveur CA Enterprise Log Manager crée une sauvegarde, puis envoie les mises à jour de contenu vers le composant incorporé du serveur de mises à jour qui stocke les mises à jour de contenu pour tous les autres serveurs CA Enterprise Log Manager.
2. En tant que client d'abonnement, le serveur CA Enterprise Log Manager installe lui-même les mises à jour des produits et du système d'exploitation dont il a besoin.

Remarque : Pour plus de détails sur la planification et la configuration de l'abonnement, consultez le *Manuel d'implémentation*. Pour plus de détails sur l'ajustement et la modification de la configuration d'abonnement et sur l'application des mises à jour aux agents, consultez le *Manuel d'administration*.

Prise en charge des adresses IP IPv6

La spécification des adresses IP était antérieurement limitée à la notation décimale IPv4, avec points. La version actuelle prend désormais en charge les adresses IPv6 dans tout champ d'adresse IP. IPv6 utilise des adresses IP de 128 bits au lieu des adresses de 32 bits utilisées par IPv4. Toute stratégie basée sur la version des adresses IP prend en charge IPv6, ainsi qu'IPv4.

Vous pouvez utiliser des adresses IPv6 mappées IPv4 ou le format IPv6 traditionnel. Le format d'adresse IPv6 mappée IPv4 permet de représenter l'adresse IPv4 d'un noeud IPv4 comme une adresse IPv6, comme suit :

- Le format IPv6 favori est rédigé sous la forme de huit groupes de quatre chiffres héxadécimaux (x:x:x:x:x:x:x:x). Chaque x correspond à quatre chiffres hexadécimaux des huit parties de 16 bits de l'adresse.
- Une adresse IPv6 mappée IPv4, très pratique dans un environnement comportant à la fois des noeuds IPv4 et IPv6, prend le format 0:0:0:0:0:FFFF:d.d.d.d, où chaque d représente une valeur décimale de l'adresse (notation décimale IPv4, avec points).

  Important : Les adresses IPv6 compatibles IPv4 au format 0:0:0:0:0:0:d.d.d.d sont maintenant abandonnées, conformément à la RFC 4291, car les mécanismes de transition IPv6 actuels n'utilisent plus ces adresses.

Voici une adresse IPv6 valide au format traditionnel.

2001:0db8:85a3:08d3:1319:8a2e:0370:7334

Si un ou plusieurs groupes de quatre chiffres sont à 0000, ces zéros peuvent être omis et remplacés par deux signes deux-points (::). Les zéros en début de groupe peuvent également être omis. Les adresses IP données en exemple ci-après sont équivalentes.

- 2001:0db8:0000:0000:0000:0000:1428:57ab
- 2001:0db8::1428:57ab
- 2001:db8:0:0:0:0:1428:57ab
- 2001:db8::1428:57ab

Si vous remplacez des adresses IPv4 par des adresses mappées IPv4, conformez-vous aux exemples ci-dessous.

- 0:0:0:0:0:FFFF:192.168.2.128
- 0:0:0:0:0:FFFF:172.16.2.128

Vous pouvez également utiliser la forme compressée présentée ci-dessous.

- ::FFFF:192.168.2.128
- ::FFFF:172.16.2.128

Chapitre 4 : Fonctionnalités r12.1 SP3 ajoutées et modifiées

La version 12.1 SP3 de CA Enterprise Log Manager contient des correctifs de bogue présents dans la version 12.1 SP2. Cette version contient la nouvelle fonctionnalité suivante :

- Installation d'un agent sur des systèmes HP-UX Itanium

Ce chapitre traite des sujets suivants :

Installation d'un agent sur des systèmes HP-UX Itanium

Vous pouvez installer un agent CA Enterprise Log Manager sur des systèmes HP-UX Itanium.

Pour obtenir des informations complémentaires sur l'installation d'un agent sur des systèmes HP-UX Itanium, consultez le *Manuel d'installation des agents*.

Chapitre 5 : Fonctionnalités r12.1 SP2 ajoutées et modifiées

Ce chapitre traite des sujets suivants :

CA Enterprise Log Manager en tant que dispositif virtuel

Vous pouvez déployer CA Enterprise Log Manager en tant que dispositif virtuel au format OVF (Open Virtualization Format). Le provisionnement du dispositif virtuel requiert moins de temps que celui d'un serveur CA Enterprise Log Manager sur un ordinateur virtuel.

Le format OVF est une norme ouverte pour le packaging et la distribution de dispositifs virtuels. CA Enterprise Log Manager utilise le format de fichier VMDK (Virtual Machine Disk) basé sur le format OVF.

Vous trouverez des informations relatives au déploiement de CA Enterprise Log Manager en tant que dispositif virtuel dans le *Manuel d'implémentation.*

Administration d'agent simplifiée

Cette fonctionnalité mise à jour simplifie le provisionnement d'un nouveau serveur CA Enterprise Log Manager. Elle permet d'effectuer les opérations suivantes :

- Mise à jour d'une liste de serveurs CA Enterprise Log Manager au niveau de l'explorateur d'agent ou d'un groupe d'agents individuel.
- Ajout d'un serveur à une liste de serveurs existante et mise à jour par CA Enterprise Log Manager de la liste de serveurs pour chaque agent.

Le *Manuel d'administration* et l'*Aide en ligne* contiennent des informations complémentaires sur le sujet.

Contrôle d'accès basé sur les rôles dans les appels de connexion API

Vous pouvez effectuer un contrôle de l'accès basé sur les rôles d'un utilisateur connecté à CA Enterprise Log Manager via l'API. Vous pouvez définir les filtres d'accès aux données appliqués à la requête au format XML. Cette spécification permet de filtrer un résultat de requête ou de rapport en fonction du rôle, lors de l'authentification à l'aide d'un nom et d'un mot de passe de certificat.

Le *Manuel de programmation de l'API* contient des informations à propos du filtre d'accès XML.

Fichiers d'aide LogSensor

Cette version contient un manuel de LogSensor pour chaque détecteur de journal. Celui-ci est accessible à partir de l'assistant d'intégration de l'interface utilisateur.

Conservation d'une configuration de rapport

Pour conserver la configuration d'un rapport, dans l'assistant de planification de rapports, sélectionnez l'option Conserver après expiration. Une fois le rapport généré, vous pouvez modifier sa configuration et le replanifier. Cette fonctionnalité est valide pour les rapports à exécution unique et les rapport à exécution immédiate.

Le *Manuel d'administration* et l'*Aide en ligne* contiennent des informations complémentaires sur le sujet.

Chapitre 6 : Fonctionnalités r12.1 SP1 ajoutées et modifiées

Ce chapitre traite des sujets suivants :

Conformité à la norme FIPS 140-2

La norme FIPS (Federal Information Processing Standards) 140-2 est une norme de sécurité pour les bibliothèques cryptographiques et pour les algorithmes qu'un produit doit utiliser pour le chiffrement. Le chiffrement FIPS 140-2 affecte la communication de toutes les données sensibles entre des composants de produits CA et entre des produits CA et des produits tiers. La norme FIPS 140-2 indique la configuration requise pour utiliser des algorithmes cryptographiques dans un système de sécurité protégeant les données sensibles et non classifiées.

CA Enterprise Log Manager offre la compatibilité avec la norme FIPS pour le trafic sécurisé d'événements utilisant des algorithmes conformes à la norme FIPS lors du fonctionnement en mode FIPS. CA Enterprise Log Manager offre également le mode par défaut non FIPS avec lequel le trafic des événements n'est *pas* sécurisé avec les algorithmes conformes à la norme FIPS. Les serveurs CA Enterprise Log Manager d'un réseau fédéré ne peuvent pas utiliser ces deux modes simultanément. Cela signifie qu'un serveur en mode non FIPS ne peut pas partager de requête et de données de rapport avec un serveur fonctionnant en mode FIPS.

Les informations concernant l'activation et la désactivation du mode FIPS sont disponibles dans le *Manuel d'implémentation*, dans la section relative à l'installation de CA Enterprise Log Manager, ainsi que dans l'aide en ligne du service Etat du système.

Informations complémentaires :

Modes de fonctionnement (page 38)
Bibliothèques de chiffrement (page 39)
Algorithmes utilisés (page 39)
Certificats et fichiers clés (page 40)
Limitations de la prise en charge de la norme FIPS (page 42)
Configuration de Microsoft Internet Explorer pour l'accès à CA Enterprise Log Manager en mode FIPS (page 43)
Configuration de Mozilla Firefox pour l'accès à CA Enterprise Log Manager en mode FIPS (page 44)

Modes de fonctionnement

CA Enterprise Log Manager peut fonctionner dans deux modes : mode FIPS et mode non FIPS. Les limites cryptographiques sont les mêmes dans les deux modes, mais les algorithmes sont différents. Par défaut, les serveurs CA Enterprise Log Manager fonctionnent en mode non FIPS. Les utilisateurs possédant le rôle d'administrateur peuvent activer le mode FIPS.

Mode non FIPS

Ce mode mélange des algorithmes de chiffrement pour le transport d'événements et pour les autres communications réalisées entre le serveur CA Enterprise Log Manager et CA EEM qui ne respectent pas forcément les normes FIPS 140-2.

Mode FIPS

Ce mode utilise des algorithmes de chiffrement certifiés FIPS pour le transport d'événements et pour les autres communications réalisées entre le serveur CA Enterprise Log Manager et CA EEM.

Les utilisateurs de niveau administrateur peuvent vérifier les modes de fonctionnement de l'agent dans le noeud Explorateur d'agent de l'onglet Administration, sous-onglet Collecte de journaux.

Pour plus d'informations concernant le passage du mode FIPS au mode non FIPS et inversement, consultez l'aide en ligne, à la rubrique consacrée aux tâches relatives à l'état du système, ou le *Manuel d'implémentation*, à la section concernant la configuration des services.

Bibliothèques de chiffrement

La norme FIPS (Federal Information Processing Standards) 140-2 indique les conditions requises pour l'utilisation des algorithmes cryptographiques dans un système de sécurité protégeant les données sensibles et non classifiées.

CA Enterprise Log Manager intègre également la bibliothèque cryptographique Crypto-C Micro Edition (ME) v2.1.0.2 de RSA, qui a été validée comme conforme les *Conditions de sécurité requises pour les modules cryptographiques* établies par la norme FIPS 140-2. Le numéro de certificat de validation de ce module est 865.

Algorithmes utilisés

Les produits logiciels qui utilisent des modules cryptographiques accrédités par la norme FIPS 140-2 dans leur mode accrédité par la norme FIPS peuvent uniquement utiliser les fonctions de sécurité approuvées par la norme FIPS, telles que AES (algorithme de chiffrement supérieur), SHA-1 (algorithme de hachage sécurisé), et des protocoles de niveau supérieur tels que TLS v1.0, tel que explicitement autorisé dans les normes FIPS 140-2 et dans les manuels d'implémentation.

En mode non FIPS, CA Enterprise Log Manager utilise les algorithmes suivants :

- AES 128
- Triple DES (3DES)
- SHA-1
- MD5
- SSL v3

En mode FIPS, CA Enterprise Log Manager utilise les algorithmes suivants :

- AES 128
- Triple DES (3DES)
- SHA-1
- TLS v1

CA Enterprise Log Manager utilise SHA-1 comme algorithme Digest par défaut pour chiffrer les mots de passe et signer les demandes de serveur.

CA Enterprise Log Manager utilise TLS v1.0 pour la communication avec des annuaires LDAP externes si la connexion LDAP se fait sur TLS, pour la communication entre les composants iTechnology, pour la communication entre l'agent et le service iGateway en mode FIPS et pour le canal d'événements entre un agent et le service logDepot.

Certificats et fichiers clés

Pour la prise en charge de FIPS 140-2, la mise à niveau vers CA Enterprise Log Manager r12.1 SP1 convertit les certificats utilisant le format P12 en certificats utilisant format PEM. Cette conversion aboutit à la génération des fichiers suivants :

- Fichier de certificat avec une extension .cer
- Fichier de clé avec une extension .key

Les fichiers de clé ne sont pas chiffrés et l'utilisateur peut décider d'en sécuriser l'accès sur les hôtes de serveur et d'agent. Le dispositif logiciel CA Enterprise Log Manager utilise plusieurs techniques de durcissement des systèmes d'exploitation pour protéger les clés et les certificats stockés dans le système de fichiers. CA Enterprise Log Manager ne prend pas en charge l'utilisation d'unités de stockage de clés externes.

CA Enterprise Log Manager utilise les certificats et les fichiers de clé suivants :

Nom de certificat/fichier clé	Emplacement	Description
CAELMCert	/opt/CA/SharedComponents/iTechnology (Vous pouvez utiliser le nom variable court ($IGW_LOC) pour accéder à ce répertoire.)	Tous les services CA Enterprise Log Manager utilisent ce certificat pour les communications entre serveurs CA Enterprise Log Manager et entre les serveurs CA Enterprise Log Manager et le serveur CA EEM. Le fichier de configuration CALM.cnf contient une entrée pour ce certificat et pour le fichier de clé correspondant. Les paires de balises commencent par <Certificate> et par <KeyFile> respectivement.
CAELM_AgentCert	$IGW_LOC sur le serveur hôte d'agent	Les agents utilisent ce certificat pour communiquer avec les serveurs CA Enterprise Log Manager. Le serveur de gestion CA Enterprise Log Manager fournit ce certificat à l'agent. Le certificat est valide uniquement pour les serveurs CA Enterprise Log Manager d'une instance d'application donnée.
itpamcert	Serveur CA IT PAM	Ce certificat est utilisé pour les communications avec CA IT PAM. Pour plus d'informations, consultez la documentation relative à CA IT PAM.
rootcert	$IGW_LOC	Ce certificat est un certificat racine signé par iGateway pendant l'installation.
iPozDsa	$IGW_LOC	Le serveur CA EEM, aussi bien local que distant, utilise ce certificat. Pour plus d'informations, reportez-vous à la documentation CA EEM.
iPozRouterDsa	$IGW_LOC	Le serveur CA EEM, aussi bien local que distant, utilise ce certificat. Pour plus d'informations, reportez-vous à la documentation CA EEM.

Nom de certificat/fichier clé	Emplacement	Description
iTechPoz-trusted	/opt/CA/Directory/dxserver/config/ssld	CA Directory utilise ce certificat.
iTechPoz-<nom_hôte>-Router	/opt/CA/Directory/dxserver/config/ssld	CA Directory utilise ce certificat.

Limitations de la prise en charge de la norme FIPS

Les fonctionnalités CA Enterprise Log Manager suivantes et les interopérations de produit ne prennent pas en charge les opérations en mode FIPS :

Accès d'ODBC et de JDBC au magasin de journaux d'événements

ODBC et JDBC sous CA Enterprise Log Manager utilise un SDK sous-jacent qui ne prend pas en charge les opérations en mode FIPS. Les administrateurs de réseaux fédérés qui exigent des opérations FIPS doivent désactiver manuellement le service ODBC sur chaque serveur CA Enterprise Log Manager. Consultez le *Manuel d'implémentation*, à la section relative à la désactivation de l'accès d'ODBC et de JDBC au magasin de journaux d'événements.

Partage d'un serveur CA EEM

CA Enterprise Log Manager r12.1 SP1 utilise CA EEM r8.4 SP3, qui est compatible avec la norme FIPS. L'activation du mode FIPS sur le serveur CA Enterprise Log Manager désactive la communication entre le produit CA EEM partagé et les produits qui ne prennent pas en charge CA EEM r8.4 SP3.

CA IT PAM, par exemple, n'est pas compatible avec la norme FIPS. Si vous procédez à la mise à niveau de votre serveur CA Enterprise Log Manager vers le mode FIPS, un échec d'intégration avec CA IT PAM se produit.

Vous pouvez partager un serveur CA EEM entre CA Enterprise Log Manager r12.1 SP1 et CA IT PAM r2.1 SP2 et r2.1 SP3 uniquement en mode non FIPS.

Si votre installation de CA IT PAM ne partage pas le même serveur CA EEM, CA Enterprise Log Manager r12.1 SP1 peut s'exécuter en mode FIPS et il peut communiquer avec CA IT PAM ; toutefois, ces canaux de communication ne sont pas compatibles avec la norme FIPS.

Correspondance des modes de fonctionnement requise pour les liaisons LDAP

La réussite de la communication avec un magasin d'utilisateurs externes dépend de ce qui suit :

- Les serveurs CA Enterprise Log Manager et leur serveur CA EEM de gestion doivent fonctionner dans le même mode FIPS.
- Si vous utilisez TLS v 1.0 pour la connexion, le serveur CA EEM doit fonctionner dans le même mode FIPS qu'un magasin d'utilisateurs externes sur lequel la norme FIPS est activée.

  Remarque : La compatibilité avec la norme FIPS n'est pas disponible lors de l'utilisation de communications non chiffrées entre le serveur CA EEM et le magasin d'utilisateurs externes ou lorsque le serveur CA EEM et le magasin d'utilisateurs fonctionnent dans des modes FIPS différents.

Interruptions SNMP

Vous pouvez utiliser SNMP V2 ou SNMP V3 pour envoyer des événements SNMP. Les deux sont pris en charge en mode non FIPS.

Si la norme FIPS est activée sur le serveur de destination des interruptions SNMP, vous devez activer la sécurité V3, puis choisir SHA comme protocole d'authentification et AES comme protocole de chiffrement. Effectuez ces sélections dans la page Destination de l'assistant de planification des alertes d'action.

Configuration de Microsoft Internet Explorer pour l'accès à CA Enterprise Log Manager en mode FIPS

Lorsque le mode FIPS est activé, des opérations de configuration supplémentaires peuvent s'avérer nécessaires pour pouvoir afficher l'interface utilisateur du serveur CA Enterprise Log Manager dans votre navigateur. Utilisez la procédure suivante pour définir les options obligatoires pour accéder à CA Enterprise Log Manager dans Microsoft Internet Explorer 7 ou 8.

Remarque : L'accès à un serveur CA Enterprise Log Manager fonctionnant en mode FIPS n'est pas possible dans Microsoft Internet Explorer 6.

Configuration de Microsoft Internet Explorer 7 ou 8

1. Ouvrez le navigateur et sélectionnez Outils, Options Internet.
2. Sélectionnez l'onglet Avancé et descendez jusqu'à la section Sécurité.

3. Sélectionnez l'une des options suivantes :
   - Utiliser SSL 2.0
   - Utiliser SSL 3.0
   - Utiliser TLS 1.0
4. Cliquez sur OK.

Configuration de Mozilla Firefox pour l'accès à CA Enterprise Log Manager en mode FIPS

Lorsque le mode FIPS est activé, des opérations de configuration supplémentaires peuvent s'avérer nécessaires pour pouvoir afficher l'interface utilisateur du serveur CA Enterprise Log Manager dans votre navigateur. Pour définir les options d'accès à un serveur CA Enterprise Log Manager fonctionnant en mode FIPS dans Mozilla Firefox 3.5.8 (ou version ultérieure), utilisez la procédure suivante.

Remarque : L'accès à CA Enterprise Log Manager requiert l'installation du module d'extension Mozilla Firefox pour Adobe Flash 9 ou 10.

Pour configurer Mozilla Firefox :

1. Ouvrez le navigateur et sélectionnez Tools (Outils), Options.
2. Cliquez sur l'onglet Advanced (Avancé), puis sur le sous-onglet Encryption (Chiffrement).
3. Sélectionnez les deux options suivantes :
   - Utiliser SSL 3.0
   - Utiliser TLS 1.0
4. Sélectionnez le sous-onglet Security (Sécurité), puis indiquez que vous souhaitez utiliser un Master Password (Mot de passe principal).
5. Cliquez sur Change Master Password (Modifier le mot de passe principal) et entrez un mot de passe dans la fenêtre qui s'affiche, puis cliquez sur OK.
6. Cliquez sur le sous-onglet Advanced (Avancé).
7. Cliquez sur Security Devices (Périphériques de sécurité).

   La fenêtre Device Manager (Gestionnaire de périphériques) s'affiche.

8. Sélectionnez le module NSS Internal PKCS #11 (PKCS #11 interne NSS) dans le volet gauche.

   Cette action remplit les données du volet droit.

9. Sélectionnez la ligne NSS Internal PKCS #11 Module et cliquez sur Enable FIPS.
10. Lorsque vous y êtes invité, saisissez le mot de passe principal que vous avez créé précédemment, puis cliquez sur OK.
11. Dans la fenêtre Device Manager (Gestionnaire d'unités), cliquez sur OK.
12. Pour fermer la boîte de dialogue Options, cliquez sur OK.
13. Redémarrez le navigateur.

Informations complémentaires :

Mise à niveau par abonnement (page 11)

Image ISO pour de nouvelles installations

Le Service Pack comprend une image ISO que vous permettra de déployer rapidement CA Enterprise Log Manager ou d'ajouter un nouveau serveur CA Enterprise Log Manager à un déploiement existant. L'image ISO est disponible dans la section Downloads (Téléchargements) sur le site du support en ligne.

Nous vous recommandons d'utiliser l'image ISO la plus récente dans les cas suivants :

- Déploiement de CA Enterprise Log Manager. L'installation de l'image ISO la plus récente permet de réduire le nombre de mises à niveau des souscriptions requises et d'accélérer le déploiement.
- Ajout d'un nouveau serveur CA Enterprise Log Manager après la mise à niveau des serveurs dans un déploiement existant. Indiquez d'abord que les serveurs et les agents du déploiement actuel sont correctement mis à niveau et qu'ils reçoivent correctement les événements. Installez ensuite les nouveaux serveurs au moyen de l'image ISO pour augmenter les capacités et réduire le nombre de mises à jour des souscriptions requises.

Remarque : La procédure d'installation a été modifiée. Une nouvelle invite vous demande si vous voulez effectuer une installation en activant le mode FIPS. Lorsque vous ajoutez un nouveau serveur CA Enterprise Log Manager à un déploiement FIPS existant (le serveur de gestion CA Enterprise Log Manager ou le serveur CA EEM distant utilisent le mode FIPS), activez le mode FIPS pendant l'installation. Si vous n'activez pas ce mode, vous ne pourrez pas enregistrer le nouveau serveur et vous devrez réinstaller. Pour plus d'informations sur le mode FIPS, consultez le *Manuel d'implémentation*.

Chapitre 7 : Fonctionnalités r12.1 ajoutées et modifiées

Ce chapitre traite des sujets suivants :

Ouvrez API Access

CA Enterprise Log Manager vous permet d'utiliser des appels d'API pour accéder à des données depuis le référentiel d'événements, à l'aide du mécanisme requête et rapport, puis de les afficher dans un navigateur Web. Vous pouvez également utiliser l'API pour intégrer des requêtes ou des rapports CA Enterprise Log Manager dans une interface CA ou d'un produit tiers.

Les fonctionnalités de l'API CA Enterprise Log Manager sont les suivantes :

- Appels API authentifiés et sécurisés
- Enregistrement de produits pour authentification unique
- Récupération d'une liste de requêtes ou de rapports filtrée à l'aide d'une balise
- Affichage d'une requête ou d'un rapport dans l'interface CA Enterprise Log Manager interactive afin de les filtrer et de les intégrer dans une interface utilisateur

Vous pouvez obtenir plus d'informations sur l'API dans le *Manuel de programmation API* et dans l'aide en ligne.

Alertes donnant lieu à une action : Intégration de CA IT PAM

Via des alertes planifiées qui interrogent les volumes d'enregistrements de journaux, CA Enterprise Log Manager détecte les éventuelles violations de contrôle et toute activité informatique suspecte. CA Enterprise Log Manager notifie le personnel chargé de la sécurité informatique qui enquête sur chaque alerte de déterminer si une action est requise pour y remédier. Les activités d'investigation typiques concernent souvent la routine et conviennent parfaitement à l'automatisation. Via une intégration étroite entre CA Enterprise Log Manager et CA IT PAM, ces actions de réponse de routine peuvent être effectuées automatiquement. Le personnel chargé de la sécurité informatique n'a pas à se charger des tâches répétitives, et peut donc se concentrer sur les problèmes les plus importants seulement.

L'intégration de CA IT PAM vous permet de créer des requêtes dans CA Service Desk, en exécutant un processus de sortie de l'événement/de l'alerte CA IT PAM prédéfini à partir des alertes. Vous pouvez aussi exécuter des processus de sortie de l'événement/de l'alerte IT PAM personnalisés depuis CA Enterprise Log Manager, qui automatisent d'autres réponses à des événements suspects.

Pour plus de détails, consultez la section "Utilisation de processus d'événement/d'alerte CA IT PAM" du chapitre Alertes d'action du *Manuel d'administration* CA Enterprise Log Manager.

Alertes pouvant être déclenchées : Intégration de SNMP avec des produits NSM

Des alertes sont générées lorsque des requêtes planifiées récupèrent des événements indiquant une activité suspecte. Vous pouvez automatiser l'envoi d'alertes de ce type sous forme d'interruptions SNMP vers des produits de surveillance de sécurité réseau, tels que CA Spectrum ou CA NSM. Vous préparez les produits de destination à recevoir et à interpréter des interruptions SNMP depuis CA Enterprise Log Manager, configurez les emplacements de destination, puis spécifiez les informations d'événement à envoyer.

Pour plus de détails, consultez la section "Utilisation d'interruptions SNMP" du chapitre Alertes d'action du *Manuel d'administration* CA Enterprise Log Manager.

Accès ODBC et JDBC

CA Enterprise Log Manager autorise l'accès en lecture seule aux informations de journal d'événements collectées, à l'aide d'ODBC et de JDBC. Vous pouvez utiliser cet accès pour effectuer des tâches comme :

- Créer des rapports clients à l'aide d'outils tels que BusinessObjects Crystal Reports
- Récupérer les informations du journal sélectionné pour une utilisation avec un moteur de corrélation
- Examiner des journaux pour détecter une intrusion ou un programme malveillant

Les fonctions d'accès ODBC et JDBC utilisent un client que vous installez sur le serveur approprié de votre réseau. Le serveur CA Enterprise Log Manager installe automatiquement ses composants côté serveur pendant la mise à jour de l'abonnement et l'installation.

Pour obtenir des informations d'installation, consultez le *Manuel d'implémentation*. Le *Manuel d'administration* contient des informations de configuration et des exemples.

Pertinence d'identité et d'actif : Intégration de CA IT PAM

L'intégration de CA IT PAM vous permet de maintenir des valeurs mises à jour pour une clé spécifique, en exécutant un traitement des valeurs dynamiques CA IT PAM. Un traitement des valeurs dynamiques est un traitement qui récupère les valeurs actuelles à partir de référentiels qui stockent des données actuelles. Si vous créez un traitement qui récupère des valeurs pour des actifs critiques à partir de votre fichier ou base de données d'actifs, vous pouvez mettre à jour la clé Critical_Assets dans des rapports et des requêtes prédéfinis en cliquant sur un bouton.

Pour plus de détails, consultez la section "Activation de l'importation de valeurs dynamiques" du chapitre Requêtes et rapports du *Manuel d'administration* CA Enterprise Log Manager.

Collecte de journal directe étendue par l'agent par défaut

Lors de l'installation de CA Enterprise Log Manager, l'écouteur Syslog, appelé Syslog_Connector, est déployé sur l'agent par défaut pour permettre la collecte d'événements Syslog. L'intégration de Linux_localsyslog, avec le connecteur associé, Linux_localsyslog_Connector, est également disponible pour collecter des événements Syslog.

L'agent par défaut peut dorénavant collecter directement des éléments autres que les événements Syslog. A l'aide du connecteur WinRm, l'agent par défaut peut collecter des événements de produits exécutés sur des plates-formes Microsoft Windows, comme les services de certificats Active Directory et Microsoft Office Communication Server. A l'aide du connecteur ODBC, l'agent par défaut peut collecter des événements depuis plusieurs bases de données, telles qu'Oracle9i et SQL Server 2005, ainsi que des applications qui stockent leurs événements dans ces bases de données.

Planification automatique des mises à jour pour les clients d'abonnement

Lors de l'installation de votre premier serveur CA Enterprise Log Manager, vous configurez des paramètres globaux pour tous les services, notamment l'abonnement. Pour les abonnements, le premier serveur que vous installez représente le proxy d'abonnement par défaut. Vous configurez l'heure de début et la fréquence de la mise à jour à laquelle ce proxy consulte le serveur d'abonnement CA pour obtenir des mises à jour. Quand vous installez des serveurs supplémentaires, ceux-ci sont, par défaut, installés en tant que clients d'abonnement. Quand vous configurez des serveurs supplémentaires, ceci doit se faire au niveau local. Vous effectuez la configuration locale en sélectionnant le nom du serveur pour configurer et ensuite annuler les configurations globales sélectionnées.

Par défaut, l'heure de début de la mise à jour des clients à abonnement est définie par le paramètre global. Quand le paramètre hérité n'est pas annulé manuellement pour forcer le retard, des problèmes surviennent. Pour empêcher ce problème, la planification des mises à jour pour les clients est désormais automatisée avec un retard de 15 minutes. La planification des mises à jour pour les clients d'abonnement n'exige plus de configuration manuelle.

Chapitre 8 : Problèmes connus

Ce chapitre traite des sujets suivants :

Agents et adaptateurs CA

Les problèmes connus relatifs aux agents et aux adaptateurs CA sont répertoriés ci-dessous.

Dépendance d'installation d'un agent sous Red Hat Linux 4

Symptôme :

Lorsque vous installez l'agent CA Enterprise Log Manager sur des systèmes Red Hat Enterprise Linux 4, l'installation échoue et affiche un message d'erreur signalant des dépendances d'installation.

Solution :

L'agent CA Enterprise Log Manager sur Red Hat Enterprise Linux 4 nécessite le package de développement logiciel. Installez cet ancien package de développement logiciel avant d'installer l'agent.

Le déploiement du connecteur en bloc avec une adresse IPv6 n'est pas correct

Symptôme :

Le déploiement de connecteurs, à partir de l'assistant Déploiement du connecteur en bloc qui fournit l'adresse du serveur au format IPV6, ne fonctionne pas comme prévu. Après un certain moment, l'état du connecteur affiche Exécution en cours. Quand vous modifiez le connecteur, vous pouvez constater que le nom du serveur n'affiche que les quatre premiers chiffres de l'adresse IPV6. Les noms d'utilisateur, mots de passe et champs du domaine s'affichent sans être renseignés.

Solution :

L'interface utilisateur CA Enterprise Log Manager envoie le contenu du fichier source en utilisant deux points doubles (::) comme délimiteur séparant chaque source. L'adresse IPv6 contenant des caractères deux points doubles (::), ceux-ci sont traités comme des délimiteurs. L'enregistrement du connecteur n'est pas enregistré correctement.

N'utilisez pas des adresses IPv6 pour effectuer un déploiement du connecteur en bloc. Vous *pouvez* utiliser des noms d'hôte pour configurer le déploiement en bloc des connecteurs. Vous pouvez également configurer un connecteur IPv6 dans l'assistant Création d'un connecteur en utilisant les instructions normales.

Echec de la configuration de la source d'événement au niveau du domaine

Symptôme :

La configuration d'un connecteur, de sorte qu'il accède à une source d'événement Windows et lise ses journaux, implique la création d'un compte d'utilisateur à faibles privilèges et l'affectation des autorisations nécessaires à celui-ci. Quand la source d'événement est un hôte Windows Server 2003 SP1, l'une des étapes consiste à définir la stratégie de sécurité locale, à savoir *Emprunter l'identité d'un client après l'authentification*. Quand ce droit d'utilisateur est défini localement, aucun problème ne survient. Cependant, si ce paramètre est appliqué comme stratégie de domaine sur tous les serveurs, l'application globale entraînera la suppression des affectations locales des autres utilisateurs, à savoir les Administrateurs et SERVICE.

Un article du support Microsoft stipule que "... les problèmes se produisent lorsqu'une stratégie de groupe qui définit que le droit d'utilisateur Emprunter l'identité d'un client après l'authentification est lié au domaine. Ce droit d'utilisateur doit être lié uniquement à un site ou à une unité d'organisation (OU)."

Solution :

Consultez l'article 930220 de la Base de connaissances Microsoft pour obtenir des conseils sur la restauration d'une connectivité TCP/IP complète en désactivant les services IPSec et en redémarrant l'ordinateur, et pour consulter les étapes permettant d'ajouter à nouveau les administrateurs et les groupes SERVICE en tant que paramètre de stratégie de groupe. Essayez le lien suivant :

http://support.microsoft.com/kb/930220/fr-fr (traduction automatique).

Microsoft recommande également les méthodes suivantes pour résoudre des problèmes provoqués par l'application du paramètre Emprunter l'identité d'un client après l'authentification en tant que stratégie de groupe :

- Méthode 1 : modifier les paramètres de la stratégie de groupe
- Méthode 2 : modifier le registre

Consultez l'article 911801 de la Base de connaissances Microsoft pour obtenir les étapes d'implémentation des deux solutions recommandées. Essayez le lien suivant :

http://support.microsoft.com/kb/911801/fr-fr (traduction automatique).

Restriction sur la configuration des ports

Symptôme :

Lorsque l'écouteur Syslog est configuré avec le port UDP par défaut sur un agent s'exécutant en tant qu'utilisateur non root sur un hôte Linux, le port UDP 514 (port par défaut pour Syslog) n'est pas ouvert et aucun événement Syslog n'est collecté sur ce port.

Solution :

Si l'agent s'exécute en tant qu'utilisateur non root sur un système UNIX, remplacez les ports de l'écouteur Syslog par des ports d'un numéro supérieur à 1 024 ou modifiez le service pour qu'il s'exécute en tant que root.

La suppression d'un serveur dans une fédération ne supprime pas l'agent par défaut

Symptôme :

Lors de la suppression d'un serveur CA Enterprise Log Manager dans un groupe de serveurs fédérés, l'agent par défaut du serveur supprimé n'est pas retiré de son groupe d'agents associé.

Solution :

Utilisez le sous-onglet Explorateur d'agent pour supprimer manuellement l'agent dans son groupe.

Les rapports sur les données collectées par le collecteur SAPI de CA n'affichent pas les événements correctement

Symptôme :

Certains champs d'événements collectés à l'aide du collecteur SAPI de CA Audit ne sont pas remplis correctement. En conséquence, la plupart des rapports ne présentent pas ces données comme prévu.

Solution :

Pour collecter les événements provenant de votre infrastructure CA Audit existante, utilisez le routeur SAPI de CA Audit.

La section Remarques pour les utilisateurs de CA Audit du *Manuel d'implémentation* contient des informations supplémentaires sur la configuration du routeur SAPI.

Arrêt de la réception d'événements par le détecteur de journaux de fichier texte sur un système d'agent Solaris

Symptôme :

Le détecteur de journaux de fichier texte cesse de recevoir des événements sur un système d'agent Solaris.

Le fichier journal du connecteur contient une erreur indiquant qu'un fichier de bibliothèque (libssl.so.0.9.7) n'a pas réussi à s'ouvrir :

```
[4] 20/07/10 18:55:50 ERROR :: [ProcessingThread::DllLoad] :Error is: ld.so.1:
caelmconnector: fatal: libssl.so.0,9.7: open failed: No such file or directory
[4] 20/07/10 18:55:50 ERROR :: [ProcessingThread::run] Dll Load and Initialize
failed, stopping the connector ...
[3] 20/07/10 18:55:50 NOTIFY :: [CommandThread::run] Cmd_Buff received is START
```

Solution :

Identifiez l'emplacement de la bibliothèque pour permettre à l'agent de recevoir des événements.

Pour résoudre l'erreur sur le système de l'agent Solaris :

1. Accédez au dossier /etc. Exemple :

   ```
   cd /etc
   ```

2. Ouvrez le fichier profile du dossier etc. Exemple :

   ```
   vi /etc/profile
   ```

3. Ajoutez les deux lignes suivantes à la fin du fichier profile :

   ```
   LD_LIBRARY_PATH=/usr/sfw/lib:$LD_LIBRARY_PATH

   export LD_LIBRARY_PATH
   ```

4. Fermez la session active dans le système de l'agent Solaris.
5. Ouvrez une nouvelle session sur le système de l'agent Solaris.
6. Arrêtez l'agent CA Enterprise Log Manager sur le système Solaris. Exemple :

   ```
   /opt/CA/ELMAgent/bin/S99elmagent stop
   ```

7. Démarrez l'agent CA Enterprise Log Manager sur le système Solaris. Exemple :

   ```
   /opt/CA/ELMAgent/bin/S99elmagent start
   ```

   Le détecteur de journaux de fichier texte commence à recevoir des événements et l'erreur ne s'affiche plus dans le fichier journal.

Capacité de réponse nulle de l'agent lors de la présence d'un nombre très élevé d'événements dans le flux

Symptôme :

Un agent CA Enterprise Log Manager ne répond plus et arrête d'accepter des événements. Le message d'erreur suivant apparaît dans le fichier caelmdispatcher.log :

```
[275] 12/07/10 14:32:05 ERROR :: FileQueue::PutEvents Unable to write to new
event file
[275] 12/07/10 14:32:05 ERROR :: WriterThread::run Unable to push events to
FileQueue, Retrying
[275] 12/07/10 14:32:10 NOTIFY :: FileQueue::UpdateCurrentWriterFile Reached Max
files configured limit=10, Not creating any new files for now
```

Solution :

Cela indique que le taux d'événements entrants pour le matériel dans l'environnement est très élevé. Vous pouvez résoudre ce problème en reconfigurant l'agent, en procédant comme suit :

1. Cliquez sur Administration, allez dans l'onglet Collecte de journaux et développez le dossier Explorateur d'agent.
2. Sélectionnez l'agent à reconfigurer, cliquez sur Modifier et réglez les paramètres suivants :

   Nombre maximum de fichiers

   Définit le nombre maximum de fichiers pouvant être créés dans la file d'attente de fichiers de réception d'événements. Le nombre maximum est limité à 1 000 fichiers. Le paramètre par défaut est 10.

   Taille maximum par fichier

   Définit la taille maximum, en Mo, pour chaque fichier de la file d'attente de fichiers de réception d'événements. Quand un fichier atteint la taille maximum, CA Enterprise Log Manager en crée un nouveau. La taille maximum est de 2048 Mo. Le paramètre par défaut est 100 Mo.

   Vous pouvez régler ces paramètres plus tard selon les besoins de votre environnement le taux d'événements par seconde.

Affichage dans l'interface utilisateur des connecteurs supprimés d'un agent

Symptôme :

Lorsque vous supprimez un connecteur d'agent, qui communique à distance avec un serveur CA Enterprise Log Manager sur lequel le serveur CA EEM est installé, le connecteur supprimé s'affiche encore dans l'interface graphique du serveur CA Enterprise Log Manager.

Solution :

Si vous mettez à jour la configuration d'un agent, CA Enterprise Log Manager requiert 5 minutes au maximum pour synchroniser le statut mis à jour de cet agent avec les autres agents d'une même fédération. Vérifiez le statut d'un connecteur supprimé après 5 minutes.

Non distribution des agents AIX, HP-UX et Solaris

Symptôme :

Lorsque vous installez CA Enterprise Log Manager r12.1 SP2 à l'aide d'une image ISO ou d'une application virtualisée, les packages d'agents AIX, HP-UX et Solaris ne sont pas distribués.

Solution :

Une fois l'installation terminée, utilisez le système d'abonnement pour télécharger les packages d'agent nécessaires.

Dispositif (hors interface utilisateur)

Les problèmes connus relatifs au dispositif logiciel (et non à l'interface utilisateur CA Enterprise Log Manager) sont répertoriés ci-dessous.

Connexion impossible au serveur CA Enterprise Log Manager sous le nom d'utilisateur EiamAdmin

Symptôme :

Le nom d'utilisateur EiamAdmin et son mot de passe ne sont pas reconnus lorsque vous tentez de vous connecter au serveur CA Enterprise Log Manager (sans utiliser l'interface utilisateur).

Solution :

Pour effectuer des tâches de maintenance, telles que la configuration de l'archivage, l'installation crée un autre nom d'utilisateur, caelmadmin, et lui affecte le même mot de passe que celui fourni à EiamAdmin par le programme d'installation. Utilisez le nom d'utilisateur caelmadmin et son mot de passe pour vous connecter au serveur CA Enterprise Log Manager.

Pour plus d'informations, consultez Comptes d'utilisateur par défaut dans le *Manuel d'implémentation*.

Ajustement d'événement

Les problèmes connus relatifs à l'ajustement d'événement sont répertoriés ci-dessous.

Une chaîne de mappage de blocs et des valeurs numériques exigent des opérateurs différents

Symptôme :

Lorsque vous utilisez l'assistant de mappage, les valeurs de mappage de blocs pour des colonnes numériques ou de chaînes de texte ne se comportent pas comme prévu.

Solution :

Lorsque vous créez des mappages de blocs, l'opérateur "Egal à" peut être utilisé uniquement sur les colonnes numériques. Utilisez l'opérateur "Correspondance" pour toutes les colonnes de chaîne de texte.

Message d'erreur généré par les règles d'analyse de message lors de leur modification

Symptôme :

Si vous copiez les règles d'abonnement et que vous essayez de modifier leur contenu, une erreur se produit.

Solution :

Cela est dû au fait que le contenu des règles d'un abonnement n'est pas trié. Si vous voulez en modifier une, vous devez repositionner toutes les règles.

Si une règle requiert une variable de mappage d'un bloc de mappage, vous devez la définir avant de l'utiliser dans ce bloc de mappage ou dans son bloc précédant. Voici l'ordre de priorité des blocs de mappage :

1. Mappage direct
2. Mappage de fonctions
3. Mappage conditionnel
4. Mappage de blocs

Requêtes et rapports

Les problèmes connus relatifs aux requêtes et aux rapports sont répertoriés ci-dessous.

Le filtre simple de l'assistant des requêtes échoue lors de l'utilisation de caractères spéciaux

Symptôme :

Les filtres simples de l'assistant des requêtes échouent quand vous saisissez des caractères spéciaux dans une valeur de champ du filtre simple. Vous pouvez enregistrer et exécuter la requête avec les caractères spéciaux suivants :

```
( ) & * > < ? : } {
```

Cependant, la requête s'exécute sans ce champ comme filtre et les données s'affichent même si la condition de correspondance échoue.

Solution :

N'utilisez pas les caractères spéciaux répertoriés dans les valeurs d'un champ du filtre simple.

Impossible de supprimer des balises qui contiennent des caractères spéciaux

Symptôme :

Les tentatives de suppression d'une requête ou d'une balise de rapport qui contient les caractères spéciaux suivants, ~ ! @ # $ % ^ & * ( ) _ + { } | : " < > ?, échouent.

Solution :

N'utilisez pas les caractères spéciaux indiqués lors de la création de balises de requête et de rapport.

Valeurs parasites dans le résultat de requêtes

Symptôme :

Lorsque vous sélectionnez une fonction SQL (excepté TRIM, TOLOWER, TOUPPER) ou le paramètre d'ordre de groupement pour une colonne, sans sélectionner le même paramètre pour les autres colonnes, le résultat de requête contient des valeurs parasites.

Solution :

Si vous sélectionnez une fonction SQL (excepté TRIM, TOLOWER et TOUPPER) ou le paramètre d'ordre de groupement pour une colonne, vous devez sélectionner le même paramètre pour les autres colonnes.

Messages d'erreur dans les pages de requête et de rapports lors du chargement de l'interface utilisateur

Symptôme :

Lorsque un serveur CA Enterprise Log Manager charge les pages de requêtes et de rapports, le message d'erreur suivant s'affiche dans l'interface utilisateur :

```
Erreur lors de l'obtention des résultats de la requête/du rapport : Erreur de
requête HTTP
```

Solution :

Cette erreur se produit si vous avez utilisé une configuration moyenne pour la collecte et des serveurs de génération de rapports utilisant CA Enterprise Log Manager en tant que dispositif virtuel. Dans un modèle de topologie en étoile, nous vous recommandons vivement d'utiliser une configuration de déploiement moyenne pour un serveur de collecte et une configuration de déploiement importante pour un serveur de génération de rapports.

Abonnement

Les problèmes connus relatifs à l'abonnement sont répertoriés ci-dessous.

Redémarrage automatique après mise à jour du SE lors d'une mise à niveau de SP

Symptôme :

Si l'option d'abonnement Redémarrage automatique après mise à jour du SE est définie sur oui lorsque vous appliquez la mise à jour du Service Pack, le système d'exploitation redémarre avant la fin de la mise à jour des fichiers binaires CA Enterprise Log Manager. En particulier, la mise à jour des scripts d'arrêt d'iGateway reste incomplète. Cette mise à jour doit être appliquée afin qu'iGateway puisse être arrêté correctement en cas de redémarrage du système d'exploitation.

Solution :

Avant d'appliquer la mise à jour de Service Pack du module Gestionnaire de journaux, définissez sur Non l'option d'abonnement Redémarrage automatique après mise à jour du SE.

Erreur de manque de mémoire sur les ordinateurs disposant de peu de mémoire

Symptôme :

Le téléchargement d'une mise à jour d'abonnement sur un ordinateur disposant de moins de mémoire que les 8 Go recommandés échoue et signale une erreur Java de manque de mémoire.

Solution :

Si vous installez CA Enterprise Log Manager sur du matériel doté de moins de 8 Go de mémoire, modifiez la taille de tas JVM.

Pour modifier la taille de tas JVM :

1. Connectez-vous au serveur CA Enterprise Log Manager en tant que caelmadmin.
2. Accédez au dossier iGateway.
3. Ouvrez le fichier caelm-java.group et localisez la section relative aux paramètres du JVM.
4. Ajoutez la nouvelle ligne, comme affichée dans l'illustration suivante en gras :

```
<JVMSettings>
              <loadjvm>true</loadjvm>
              <javahome>/usr/java/latest/jre</javahome>
              <Properties name="java.endorsed.dirs=/opt/CA/SharedComponents/iTechnology/endorsed">
                      <system-properties>java.endorsed.dirs=/opt/CA/SharedComponents/iTechnology/endorsed</system-properties>
              </Properties>
      <Properties name="maxmemory"><jvm-property>-Xmx1250M</jvm-property></Properties>
      </JVMSettings>
```

5. Enregistrez le fichier caelm-java.group, puis fermez-le.

Important : La définition de la taille du segment de mémoire JVM peut entraîner des problèmes lors de l'utilisation de l'option Exporter au format PDF sur des ensembles de données volumineux. Ainsi, cette option donne des résultats corrects uniquement sur les petits ordinateurs fonctionnant avec moins de mémoire RAM et de puissance de traitement que celles recommandées.

Apparition unique d'un événement d'autosurveillance de redémarrage

Symptôme :

Si vous sélectionnez un module de système d'exploitation à télécharger par abonnement et que vous spécifiez l'option sans redémarrage pour l'installer, l'événement d'autosurveillance suivant est généré une seule fois : Mises à jour de système d'exploitation installées sur cet hôte... Redémarrez l'ordinateur pour que ces mises à jour prennent effet.

Solution :

L'abonnement génère un événement qui vous rappelle de redémarrer le système d'exploitation une seule fois lorsqu'un redémarrage manuel est requis. Il convient de créer une alerte pour cet événement.

Gestion des utilisateurs et des accès

Les problèmes connus relatifs à la gestion des utilisateurs et des accès sont répertoriés ci-dessous.

Restriction sur l'utilisation d'un calendrier avec stratégies d'accès

Symptôme :

Vous avez limité à l'utilisateur ou au groupe l'accès à CA Enterprise Log Manager pendant les heures et les jours spécifiés sur un calendrier, avec une stratégie qui accorde explicitement l'accès. Cependant, ce calendrier ne fonctionne pas comme prévu avec une stratégie qui refuse explicitement l'accès.

Solution :

Pour limiter les heures d'accès d'un groupe, utilisez une stratégie qui accorde explicitement l'accès plutôt qu'une stratégie qui le refuse explicitement.

Divers

Les différents problèmes connus sont répertoriés ci-dessous.

Occasionnellement, CA Enterprise Log Manager ne répond pas

Symptôme :

Il arrive parfois que CA Enterprise Log Manager ne réponde plus. L'interface utilisateur ne répond pas aux demandes des utilisateurs et les demandes internes de l'agent au gestionnaire d'agent s'arrêtent. Toutefois, la collecte des journaux continue.

Solution :

Utilisez la procédure suivante pour arrêter le processus iGateway et le redémarrer :

1. Connectez-vous au serveur CA Enterprise Log Manager qui ne répond pas, au moyen de ssh et en tant qu'utilisateur caelmadmin.
2. Basculez sur le compte d'utilisateur root au moyen de la commande ci-dessous et entrez le mot de passe de l'utilisateur root.

   ```
   su -
   ```

3. Accédez au répertoire $IGW_LOC.

   Par défaut, iGateway se trouve dans le répertoire /opt/CA/SharedComponents/iTechnology.

4. Arrêtez le processus iGateway à l'aide de la commande ci-après.

   ```
   ./S99igateway stop
   ```

5. Démarrez le processus iGateway à l'aide de la commande ci-après.

   ```
   ./S99igateway start
   ```

Paramètres de contraste élevé pour l'écran

Symptôme :

Sous Windows, le seul paramètre de contraste élevé pris en charge est Contraste noir élevé ; les trois autres options de contraste élevé ne sont pas prises en charge. Les options de contraste élevé comprennent Contraste élevé 1, Contraste élevé 2, Contraste noir élevé et Contraste blanc élevé.

Solution :

Lorsqu'un paramètre de contraste élevé est nécessaire, sélectionnez Contraste noir élevé. Pour définir cette option, sélectionnez Affichage dans le Panneau de configuration. Cette option d'accessibilité est définie dans la boîte de dialogue Propriétés d'affichage, onglet Apparence, liste déroulante Modèle de couleurs.

iGateway s'arrête et redémarre continuellement

Symptôme :

L'interface CA Enterprise Log Manager se bloque occasionnellement. La vérification du serveur CA Enterprise Log Manager révèle que le processus iGateway s'arrête et redémarre mais ne réussit pas à rester en état de fonctionnement. Pour vérifier le processus iGateway, procédez comme suit :

1. Accédez à une invite de commande sur le serveur CA Enterprise Log Manager.
2. Connectez-vous en utilisant les informations d'identification du compte caelmadmin.
3. Basculez sur le compte d'utilisateur root au moyen de la commande ci-dessous.

   ```
   su - root
   ```

4. Utilisez la commande suivante pour vérifier que le processus iGateway s'exécute.

   ```
   ps -ef | grep igateway
   ```

   Le système d'exploitation renvoie les informations sur le processus iGateway, ainsi qu'une liste des processus s'exécutant sous iGateway.

Solution :

Pour contourner le problème, procédez comme suit.

1. Accédez à $IGW_LOC (/opt/CA/SharedComponents/iTechnology) et recherchez le fichier ci-dessous.

   ```
   saf_epSIM.*
   ```

   Ce fichier comporte plusieurs versions numérotées séquentiellement, par exemple saf_epSIM.1, saf_epSIM.2, saf_epSIM.3, etc.

2. Renommez le fichier de numéro de version le moins élevé, puis enregistrez-le ailleurs afin de le transmettre au support de CA.
3. Si iGateway ne redémarre pas automatiquement, redémarrez-le manuellement comme suit.
   a. Connectez-vous en tant qu'utilisateur root.
   b. Accédez à une invite de commande, puis entrez la commande ci-après.

      ```
      /opt/CA/SharedComponents/iTechnology/S99igateway start
      ```

L'espace disque maximal pour CA Enterprise Log Manager virtuel est insuffisant

Symptôme :

Il est impossible de créer un ordinateur virtuel avec un espace disque alloué de 512 Go dans VMware ESX Server v3.5. Pour traiter le volume d'événements, mon serveur virtuel CA Enterprise Log Manager nécessite davantage que le maximum de 256 Go.

Solution :

VMWare ESX Server utilise une taille de bloc par défaut de 1 Mo et calcule l'espace disque maximal à partir de cette valeur. Lorsque la taille des blocs est définie sur 1 Mo, l'espace disque maximal prend la valeur par défaut de 256 Go. Si vous souhaitez configurer plus de 256 Go d'espace disque virtuel, vous pouvez augmenter la taille de bloc par défaut.

Pour créer un disque virtuel plus grand

1. Accédez à la console de service du serveur VMware ESX Server.
2. Augmentez la taille de bloc à 2 Mo au moyen de la commande ci-dessous.

   ```
   vmkfstools --createfs vmfs3 --blocksize 2M vmhba0:0:0:3
   ```

   Dans cette commande, la valeur 2M signifie 512 Go (2 x 256).
3. Redémarrez le serveur VMware ESX Server.
4. Créez un nouvel ordinateur virtuel dont l'espace disque est défini sur 512 Go.

Pour plus d'informations sur cette commande et sur d'autres commandes, consultez la documentation VMware ESX Server.

Valeurs nulles affichées dans les champs CEG Date/Heure

Symptôme :

Si vous importez une règle de transfert avec le champ CEG Date/Heure pour transférer des événements, les champs CEG Date/Heure sont affichés dans l'interface graphique avec une valeur nulle.

Solution :

N'utilisez aucun des champs suivants dérivés du champ CEG Date/Heure pour les règles de suppression et de récapitulation et pour les règles de transfert :

- event_datetime
- event_year_datetime
- event_month_datetime
- event_day_datetime
- event_hour_datetime
- event_quarterhour_datetime
- event_minute_datetime

L'actualisation d'un navigateur déconnecte un utilisateur de CA Enterprise Log Manager

Symptôme :

Si vous actualisez votre navigateur alors que vous êtes connecté à CA Enterprise Log Manager, votre session prend fin et vous êtes déconnecté.

Solution :

CA Enterprise Log Manager ne prend pas en charge l'actualisation des navigateurs en raison de restrictions Flex. Evitez d'actualiser votre navigateur.

Erreur possible au niveau du service ou de l'interface de l'explorateur après le redémarrage d'iGateway

Symptôme :

Si vous cliquez sur un objet dans les services de l'interface CA Enterprise Log Manager ou dans les arborescences d'explorateur immédiatement après le redémarrage d'iGateway, le message d'erreur "Network error on receive" (erreur réseau lors de la réception) risque de s'afficher à la place du contenu demandé.

Solution :

Cette erreur se produit si vous essayez d'accéder à l'un des objets spécifiés pendant son rechargement après le redémarrage d'iGateway. Patientez pendant cinq minutes pour permettre le rechargement et cliquez sur les services ou sur l'élément d'explorateur de votre choix.

Echec des chargements et des exportations avec des navigateurs autres qu'Internet Explorer

Symptôme :

Si vous utilisez Mozilla Firefox, Safari ou Chrome pour accéder à CA Enterprise Log Manager, vous pourrez effectuer pratiquement toutes les tâches CA Enterprise Log Manager, sauf les tâches d'importation et de chargement. Vous trouverez plusieurs exemples ci-dessous.

- Echec de l'importation d'une définition de requête et envoi du message "Erreur d'E/S : Echec de la demande".
- Echec du chargement des fichiers CSV avec l'assistant de déploiement du connecteur en bloc, malgré l'affichage du message suivant : Veuillez patienter pendant le chargement du fichier.

Solution :

Utilisez Microsoft Internet Explorer pour accéder à CA Enterprise Log Manager afin d'importer ou de charger des fichiers.

L'affichage de l'interface utilisateur échoue de manière inattendue lors d'une installation avec un EEM distant

Symptôme :

Lors de l'installation de CA Enterprise Log Manager avec un serveur EEM distant, l'affichage de l'interface utilisateur échoue occasionnellement lors de la connexion initiale. La vérification des fichiers journaux iGateway indique que les services agentmanager, calmreporter, subscclient et subscproxy n'ont pas été démarrés.

La syntaxe du fichier journal peut s'apparenter à celle-ci :

```
[1087523728] 23/09/09 20:35:32 ERROR :: Certificate::loadp12 :
etpki_file_to_p12 failed [ errorcode : -1 ]

[1087523728] 23/09/09 20:35:32 ERROR :: Certificate::loadp12 :
etpki_file_to_p12 failed [ errorcode : -1 ]

[1087523728] 23/09/09 20:35:32 ERROR :: Certificate::loadp12 :
etpki_file_to_p12 failed [ errorcode : -1 ]

[1087527824] 23/09/09 17:00:07 ERROR ::
OutProcessSponsorManager::stopSponsorGroup : terminating safetynet process
for SponsorGroup [ caelm-msgbroker ] didn't respond OK for the termination
call

[1087527824] 23/09/09 17:00:07 ERROR ::
OutProcessSponsorManager::stopSponsorGroup : terminating safetynet process
for SponsorGroup [ caelm-oaserver ] didn't reaspond OK for the termination
call

[1087527824] 23/09/09 17:00:07 ERROR ::
OutProcessSponsorManager::stopSponsorGroup : terminating safetynet process
for SponsorGroup [ caelm-sapicollector ] didn't reaspond OK for the
termination call

[1087527824] 23/09/09 17:07:46 ERROR :: OutProcessSponsorManager::start :
SponsorGroup [ caelm-java ] failed to start ]

[1087527824] 23/09/09 17:07:49 ERROR :: SponsorManager::start : Sponsor [
agentmanager ] failed to load

[1087527824] 23/09/09 17:07:49 ERROR :: SponsorManager::start : Sponsor [
calmreporter ] failed to load

[1087527824] 23/09/09 17:07:49 ERROR :: SponsorManager::start : Sponsor [
subscclient ] failed to load

[1087527824] 23/09/09 17:07:49 ERROR :: SponsorManager::start : Sponsor [
subscproxy ] failed to load
```

Solution :

Vous pouvez résoudre ce problème en redémarrant iGateway, puis en vous reconnectant à l'interface.

Pour redémarrer le service iGateway

1. Cliquez sur l'onglet Administration, puis sur le sous-onglet Services.
2. Développez l'entrée Etat du système.
3. Sélectionnez un serveur CA Enterprise Log Manager spécifique.
4. Cliquez sur l'onglet Administration du service.
5. Cliquez sur Redémarrer iGateway.

Mise à niveau vers CA Audit requise pour l'interopérabilité avec CA Enterprise Log Manager

Symptôme :

L'installation d'un serveur CA Enterprise Log Manager utilise un serveur CA Embedded Entitlements Manager existant installé avec CA Audit r8 SP2. Lors de l'accès à l'interface utilisateur d'Audit Administrator, une tentative de modification des détails d'agent renvoie le message d'erreur :

```
"Avertissement : Aucun serveur de gestionnaire de journaux n'est disponible."
```

Tous les champs de la page Modifier les détails de l'agent d'Audit Administrator possèdent des valeurs vierges.

Cela est dû à une interaction incompatible entre le serveur r8.4 CA EEM et le client r8.4 CA EEM, présent dans CA Enterprise Log Manager r12.1. La version antérieure ne prend pas en charge une fonctionnalité appelée par le SDK plus récent.

Solution :

Pour résoudre le problème de correspondance entre les versions et utiliser CA Enterprise Log Manager avec CA Audit r8 SP2, mettez à niveau l'implémentation de CA Audit existante vers CA Audit r8 SP2 CR1. Vous pouvez ensuite utiliser les fonctionnalités de l'agent CA Enterprise Log Manager et du gestionnaire d'agent avec CA Audit.

Chapitre 9 : Problèmes résolus

Ce chapitre traite des sujets suivants :

Liste des problèmes

Les demandes d'amélioration suivantes ont été résolues dans CA Enterprise Log Manager r12.1 SP2.

- 18853365-1
- 18853310-1
- 18699660-1
- 18713453-1
- 19079108-1
- 19046629-1
- 19078906-1
- 18853408-1

Les problèmes suivants, signalés par des clients, ont été résolus dans CA Enterprise Log Manager r12.1 SP2.

- 19201526-1
- 19078767-2
- 19222906
- 19179699-1
- 19266092-1
- 19313624-1
- 19379354
- 19399295
- 19454801
- 19468531
- 19188433-7
- 19581946
- 19602784
- 19173006-1
- 18977697-1
- 19188433-4
- 19255064-1

- 19188433-3
- 19222992
- 19236219
- 19188433-5
- 19378391-1
- 19280900-1
- 19289970-1
- 19297282-1
- 19370519
- 19373496
- 19467808
- 19428046
- 19459527
- 19543395
- 19539006-1

Chapitre 10 : Documentation

Ce chapitre traite des sujets suivants :

Bibliothèque

La bibliothèque offre un accès à toute la documentation CA Enterprise Log Manager à partir d'un emplacement central. La bibliothèque offre les opportunités suivantes.

- Liste extensible des contenus de tous les manuels au format HTML
- Recherche de texte intégral dans l'ensemble des manuels, avec classement des résultats de recherche et termes recherchés mis en surbrillance dans le contenu

  Remarque : Si vous recherchez du texte purement numérique, placez un astérisque avant la valeur de recherche.
- Des chemins de navigation reliés aux rubriques du niveau supérieur
- Index unique pour tous les manuels
- Des liens vers les versions PDF des manuels pour impression

Accès à la bibliothèque

Les bibliothèques de documentation de produit CA sont disponibles pour téléchargement dans des fichiers ZIP incluant un index de recherche.

Pour accéder à la bibliothèque CA Enterprise Log Manager :

1. Allez à Rechercher dans la documentation/les manuels.
2. Entrez CA Enterprise Log Manager comme produit, sélectionnez une version et une langue, puis cliquez sur OK.
3. Téléchargez le fichier ZIP sur votre ordinateur ou à un autre emplacement.
4. Ouvrez le fichier ZIP et faites glisser le dossier de bibliothèque vers votre ordinateur ou extrayez-le à un autre emplacement.
5. Ouvrez le dossier de bibliothèque.
6. Ouvrez la bibliothèque :
   - Si la bibliothèque est située sur le système local et que vous utilisez Internet Explorer, ouvrez le fichier Bookshelf.hta.
   - Si la bibliothèque est située sur un système distant ou que vous utilisez Mozilla Firefox, ouvrez le fichier Bookshelf.html.

   La bibliothèque s'ouvre.

Annexe A : Communiqués de tiers

Ce chapitre traite des sujets suivants :

Adaptive Communication Environment (ACE) 5.5.10

Copyright and Licensing Information for ACE(TM), TAO(TM), CIAO(TM), and CoSMIC(TM)

The ACE, TAO, CIAO, and CoSMIC web sites are maintained by the DOC Group at the Institute for Software Integrated Systems (ISIS) and the Center for Distributed Object Computing of Washington University, St. Louis for the development of open-source software as part of the open-source software community. Submissions are provided by the submitter ``as is|&"&| with no warranties whatsoever, including any warranty of merchantability, noninfringement of third party intellectual property, or fitness for any particular purpose. In no event shall the submitter be liable for any direct, indirect, special, exemplary, punitive, or consequential damages, including without limitation, lost profits, even if advised of the possibility of such damages. Likewise, DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies around the world provide commercial support for DOC software, however.

DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant. Likewise, DOC software is compliant with the new US daylight savings rule passed by Congress as "The Energy Policy Act of 2005," which established new daylight savings times (DST) rules for the United States that expand DST as of March 2007. Since DOC software obtains time/date and calendaring information from operating systems users will not be affected by the new DST rules as long as they upgrade their operating systems accordingly.

The names ACE(TM), TAO(TM), CIAO(TM), CoSMIC(TM), Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. This license grants no permission to call products or services derived from this source ACE(TM), TAO(TM), CIAO(TM), or CoSMIC(TM), nor does it grant permission for the name Washington University, UC Irvine, or Vanderbilt University to appear in their names.

If you have any suggestions, additions, comments, or questions, please let me know.

Douglas C. Schmidt

Software under the Apache License

Ce produit utilise les logiciels Apache suivants :

- Ant 1.6.5
- Formatting Objects Processor (FOP) 0.95
- Jakarta POI 3.0
- Log4cplus 1.0.2
- Log4j 1.2.15
- Qpid 0.5.0
- Qpid 0.6.0
- Quartz 1.5.1
- Super CSV 1.52
- Xerces-C 2.6.0
- XMLBeans 2.5.0

Certaines parties de ce produit comprennent des logiciels développés par Apache Software Foundation. Les logiciels Apache sont distribués conformément au contrat de licence suivant.

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

'License' shall mean the terms and conditions for use, reproduction,and distribution as defined by Sections 1 through 9 of this document.

'Licensor' shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

'Legal Entity' shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, 'control' means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

'You' (or 'Your') shall mean an individual or Legal Entity exercising permissions granted by this License.

'Source' form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

'Object' form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and versions to other media types.

'Work' shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work(an example is provided in the Appendix below).

'Derivative Works' shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

'Contribution' shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, 'submitted' means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as 'Not a Contribution.'

'Contributor' shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s)with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a 'NOTICE' text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an 'AS IS' BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Boost 1.39.0

Ce produit inclut Boost v.1.39.0, distribué conformément à la licence suivante :

DataDirect OpenAccess 6.0

The Licensed Program contains the technology OpenAccess ODBC from Progress Software Corporation ("Progress") for which the following applies. In no event will Progress or its suppliers be liable for any damages including direct, special, consequential, and indirect damages.

JDOM 1.0

Ce produit comprend du logiciel développé par JDOM Project (http://www.jdom.org/). Le logiciel JDOM est distribué conformément au contrat de licence suivant.

This software consists of voluntary contributions made by many individuals on behalf of the JDOM Project and was originally created by Jason Hunter and Brett McLaughlin. For more information on the JDOM Project, please see http://www.jdom.org.

Red Hat Enterprise Linux 5.5

This CA product is distributed with Red Hat Enterprise Linux Version 5.5 (the "Red Hat Software"), the use of which is governed by the following terms:

The Red Hat Software is open source software that is used with this CA software program (the "CA Product"). The Red Hat Software is not owned by CA, Inc. ("CA"). Use, copying, distribution and modification of the Red Hat Software are governed by the End User License Agreement Red Hat Enterprise Linux and Red Hat Applications ("Red Hat License") and related license agreements referenced therein, including the GNU General Public License version 2 (the "GPL"). A copy of the GPL license can be found in a directory within the Red Hat Software. Additionally, a copy of the GPL license can be found at http://www.gnu.org/licenses/gpl-2,0.html or write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA. Les termes du contrat de licence de Red Hat sont exposés ci-après. CA met à votre disposition le code source du logiciel Red Hat à l'adresse : http://opensrcd.ca.com/ips/04237_5/. Use of the CA Product is governed solely by the CA end user license agreement ("EULA"), not by the Red Hat License or the GPL license. You cannot use, copy, modify or redistribute any CA Product code except as may be expressly set forth in the EULA. The Red Hat Software is provided 'AS IS' WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Further details of the disclaimer of warranty with respect to the Red Hat Software can be found in the Red Hat License and in the GPL license itself. To the full extent permitted under applicable law, CA disclaims all warranties and liability arising from or related to any use of the Red Hat Software.

LICENSE AGREEMENT

RED HAT® ENTERPRISE LINUX®

AND RED HAT® APPLICATIONS

This end user license agreement ("EULA") governs the use of any of the versions of Red Hat Enterprise Linux, any Red Hat Applications (as set forth at www.redhat.com/licenses/products), and any related updates, source code, appearance, structure and organization (the "Programs"), regardless of the delivery mechanism.

1. License Grant. Subject to the following terms, Red Hat, Inc. ("Red Hat") grants to you ("User") a perpetual, worldwide license to the Programs pursuant to the GNU General Public License v.2. The Programs are either a modular operating system or an application consisting of hundreds of software components. With the exception of certain image files identified in Section 2 below, the license agreement for each software component is located in the software component's source code and permits User to run, copy, modify, and redistribute (subject to certain obligations in some cases) the software component, in both source code and binary code forms. This EULA pertains solely to the Programs and does not limit User's rights under, or grant User rights that supersede, the license terms of any particular component.

2. Intellectual Property Rights. The Programs and each of their components are owned by Red Hat and others and are protected under copyright law and under other laws as applicable. Title to the Programs and any component, or to any copy, modification, or merged portion shall remain with the aforementioned, subject to the applicable license. The "Red Hat" trademark and the "Shadowman" logo are registered trademarks of Red Hat in the U.S. and other countries. This EULA does not permit User to distribute the Programs or their components using Red Hat's trademarks, regardless of whether the copy has been modified. User should read the information found at http://www.redhat.com/about/corporate/trademark/ before distributing a copy of the Programs. User may make a commercial redistribution of the Programs only if, (a) a separate agreement with Red Hat authorizing such commercial redistribution is executed or other written permission is granted by Red Hat or (b) User modifies any files identified as "REDHAT-LOGOS" to remove and replace all images containing the "Red Hat" trademark or the "Shadowman" logo. Merely deleting these files may corrupt the Programs.

3. Limited Warranty. Except as specifically stated in this Section 3, a separate agreement with Red Hat, or a license for a particular component, to the maximum extent permitted under applicable law, the Programs and the components are provided and licensed "as is" without warranty of any kind, expressed or implied, including the implied warranties of merchantability, non-infringement or fitness for a particular purpose. Red Hat warrants that the media on which the Programs and the components are furnished will be free from defects in materials and manufacture under normal use for a period of 30 days from the date of delivery to User. Red Hat does not warrant that the functions contained in the Programs will meet User's requirements or that the operation of the Programs will be entirely error free, appear precisely as described in the accompanying documentation, or comply with regulatory requirements. This warranty extends only to the party that purchases services pertaining to the Programs from Red Hat or a Red Hat authorized distributor.

4. Limitation of Remedies and Liability. To the maximum extent permitted by applicable law, User's exclusive remedy under this EULA is to return any defective media within 30 days of delivery along with a copy of User's payment receipt and Red Hat, at its option, will replace it or refund the money paid by User for the media. To the maximum extent permitted under applicable law, neither Red Hat, any Red Hat authorized distributor, nor the licensor of any component provided to User under this EULA will be liable to User for any incidental or consequential damages, including lost profits or lost savings arising out of the use or inability to use the Programs or any component, even if Red Hat, such authorized distributor or licensor has been advised of the possibility of such damages. In no event shall Red Hat's liability, an authorized distributor's liability or the liability of the licensor of a component provided to User under this EULA exceed the amount that User paid to Red Hat under this EULA during the twelve months preceding the action.

5. Export Control. As required by the laws of the United States and other countries, User represents and warrants that it: (a) understands that the Programs and their components may be subject to export controls under the U.S. Commerce Department's Export Administration Regulations ("EAR"); (b) is not located in a prohibited destination country under the EAR or U.S. sanctions regulations (currently Cuba, Iran, Iraq, North Korea, Sudan and Syria, subject to change as posted by the United States government); (c) will not export, re-export, or transfer the Programs to any prohibited destination or persons or entities on the U.S. Bureau of Industry and Security Denied Parties List or Entity List, or the U.S. Office of Foreign Assets Control list of Specially Designated Nationals and Blocked Persons, or any similar lists maintained by other countries, without the necessary export license(s) or authorizations(s); (d) will not use or transfer the Programs for use in connection with any nuclear, chemical or biological weapons, missile technology, or military end-uses where prohibited by an applicable arms embargo, unless authorized by the relevant government agency by regulation or specific license; (e) understands and agrees that if it is in the United States and exports or transfers the Programs to eligible end users, it will, to the extent required by EAR Section 740,17(e), submit semi-annual reports to the Commerce Department's Bureau of Industry and Security, which include the name and address (including country) of each transferee; and (f) understands that countries including the United States may restrict the import, use, or export of encryption products (which may include the Programs and the components) and agrees that it shall be solely responsible for compliance with any such import, use, or export restrictions.

6. Third Party Programs. Red Hat may distribute third party software programs with the Programs that are not part of the Programs. These third party programs are not required to run the Programs, are provided as a convenience to User, and are subject to their own license terms. The license terms either accompany the third party software programs or can be viewed at http://www.redhat.com/licenses/thirdparty/eula.html. If User does not agree to abide by the applicable license terms for the third party software programs, then User may not install them. If User wishes to install the third party software programs on more than one system or transfer the third party software programs to another party, then User must contact the licensor of the applicable third party software programs.

7. Général If any provision of this agreement is held to be unenforceable, that shall not affect the enforceability of the remaining provisions. This agreement shall be governed by the laws of the State of New York and of the United States, without regard to any conflict of laws provisions. The rights and obligations of the parties to this EULA shall not be governed by the United Nations Convention on the International Sale of Goods.

SNMP4J 1.9.3d

Ce produit inclut le logiciel SNMP4J 1.9.3d et est distribué conformément au contrat de licence suivant.

'Derivative Works' shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

'Contribution' shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, 'submitted' means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as 'Not a Contribution.'

'Contributor' shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s)with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a 'NOTICE' text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an 'AS IS' BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Sun JDK 1.6.0_7

This Product is distributed with Sun JDK 1.6.0_7 (JAVA SE DEVELOPMENT KIT (JDK), VERSION 6) (Sun JDK). The Sun JDK is distributed in accordance with the Sun Microsystems, Inc. (Sun) Binary Code License Agreement set forth below. As noted in Section G of the Supplemental License Terms of this license, Sun has provided additional copyright notices and license terms that may be applicable to portions of the Sun JDK in the THIRDPARTYLICENSEREADME.txt file that accompanies the Sun JDK.

Sun Microsystems, Inc. Binary Code License Agreement for the JAVA SE DEVELOPMENT KIT (JDK), VERSION 6

SUN MICROSYSTEMS, INC. ("SUN") IS WILLING TO LICENSE THE SOFTWARE IDENTIFIED BELOW TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS BINARY CODE LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY "AGREEMENT"). PLEASE READ THE AGREEMENT CAREFULLY. BY DOWNLOADING OR INSTALLING THIS SOFTWARE, YOU ACCEPT THE TERMS OF THE AGREEMENT. INDICATE ACCEPTANCE BY SELECTING THE "ACCEPT" BUTTON AT THE BOTTOM OF THE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY ALL THE TERMS, SELECT THE "DECLINE" BUTTON AT THE BOTTOM OF THE AGREEMENT AND THE DOWNLOAD OR INSTALL PROCESS WILL NOT CONTINUE.

1. DEFINITIONS. "Software" means the identified above in binary form, any other machine readable materials (including, but not limited to, libraries, source files, header files, and data files), any updates or error corrections provided by Sun, and any user manuals, programming guides and other documentation provided to you by Sun under this Agreement. "General Purpose Desktop Computers and Servers" means computers, including desktop, laptop and tablet computers, or servers, used for general computing functions under end user control (such as but not specifically limited to email, general purpose Internet browsing, and office suite productivity tools).

The use of Software in systems and solutions that provide dedicated functionality (other than as mentioned above) or designed for use in embedded or function-specific software applications, for example but not limited to: Software embedded in or bundled with industrial control systems, wireless mobile telephones, wireless handheld devices, kiosks, TV/STB, Blu-ray Disc devices, telematics and network control switching equipment, printers and storage management systems, and other related systems are excluded from this definition and not licensed under this Agreement. "Programs" means Java technology applets and applications intended to run on the Java Platform Standard Edition (Java SE) platform on Java-enabled General Purpose Desktop Computers and Servers.

2. LICENSE TO USE. Subject to the terms and conditions of this Agreement, including, but not limited to the Java Technology Restrictions of the Supplemental License Terms, Sun grants you a non-exclusive, non-transferable, limited license without license fees to reproduce and use internally Software complete and unmodified for the sole purpose of running Programs. Additional licenses for developers and/or publishers are granted in the Supplemental License Terms.

3. RESTRICTIONS. Software is confidential and copyrighted. Title to Software and all associated intellectual property rights is retained by Sun and/or its licensors. Unless enforcement is prohibited by applicable law, you may not modify, decompile, or reverse engineer Software. You acknowledge that Licensed Software is not designed or intended for use in the design, construction, operation or maintenance of any nuclear facility. Sun Microsystems, Inc. disclaims any express or implied warranty of fitness for such uses. No right, title or interest in or to any trademark, service mark, logo or trade name of Sun or its licensors is granted under this Agreement. Additional restrictions for developers and/or publishers licenses are set forth in the Supplemental License Terms.

4. LIMITED WARRANTY. Sun warrants to you that for a period of ninety (90) days from the date of purchase, as evidenced by a copy of the receipt, the media on which Software is furnished (if any) will be free of defects in materials and workmanship under normal use. Except for the foregoing, Software is provided "AS IS". Your exclusive remedy and Sun's entire liability under this limited warranty will be at Sun's option to replace Software media or refund the fee paid for Software. Any implied warranties on the Software are limited to 90 days. Some states do not allow limitations on duration of an implied warranty, so the above may not apply to you. This limited warranty gives you specific legal rights. You may have others, which vary from state to state.

5. DISCLAIMER OF WARRANTY. UNLESS SPECIFIED IN THIS AGREEMENT, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT THESE DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

6. LIMITATION OF LIABILITY. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event will Sun's liability to you, whether in contract, tort (including negligence), or otherwise, exceed the amount paid by you for Software under this Agreement. The foregoing limitations will apply even if the above stated warranty fails of its essential purpose. Some states do not allow the exclusion of incidental or consequential damages, so some of the terms above may not be applicable to you.

7. TERMINATION. This Agreement is effective until terminated. You may terminate this Agreement at any time by destroying all copies of Software. This Agreement will terminate immediately without notice from Sun if you fail to comply with any provision of this Agreement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right. Upon Termination, you must destroy all copies of Software.

8. EXPORT REGULATIONS. All Software and technical data delivered under this Agreement are subject to US export control laws and may be subject to export or import regulations in other countries. You agree to comply strictly with all such laws and regulations and acknowledge that you have the responsibility to obtain such licenses to export, re-export, or import as may be required after delivery to you.

9. TRADEMARKS AND LOGOS. You acknowledge and agree as between you and Sun that Sun owns the SUN, SOLARIS, JAVA,JINI, FORTE, and iPLANET trademarks and all SUN, SOLARIS, JAVA, JINI, FORTE, and iPLANET-related trademarks, service marks, logos and other brand designations ("Sun Marks"), and you agree to comply with the Sun Trademark and Logo Usage Requirements currently located at http://www.sun.com/policies/trademarks. Any use you make of the Sun Marks inures to Sun's benefit.

10. U.S. GOVERNMENT RESTRICTED RIGHTS. If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation will be only as set forth in this Agreement; this is in accordance with 48 CFR 227,7201 through 227,7202-4 (for Department of Defense (DOD) acquisitions) and with 48 CFR 2,101 and 12,212 (for non-DOD acquisitions).

11. GOVERNING LAW. Any action related to this Agreement will be governed by California law and controlling U.S. federal law. No choice of law rules of any jurisdiction will apply.

12. SEVERABILITY. If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.

13. INTEGRATION. This Agreement is the entire agreement between you and Sun relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

SUPPLEMENTAL LICENSE TERMS

These Supplemental License Terms add to or modify the terms of the Binary Code License Agreement. Capitalized terms not defined in these Supplemental Terms shall have the same meanings ascribed to them in the Binary Code License Agreement. These Supplemental Terms shall supersede any inconsistent or conflicting terms in the Binary Code License Agreement, or in any license contained within the Software.

R. Software Internal Use and Development License Grant. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software "README" file incorporated herein by reference, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce internally and use internally the Software complete and unmodified for the purpose of designing, developing, and testing your Programs.

B. License to Distribute Software. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software README file, including, but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute the Software, provided that (i) you distribute the Software complete and unmodified and only bundled as part of, and for the sole purpose of running, your Programs, (ii) the Programs add significant and primary functionality to the Software, (iii) you do not distribute additional software intended to replace any component(s) of the Software, (iv) you do not remove or alter any proprietary legends or notices contained in the Software, (v) you only distribute the Software subject to a license agreement that protects Sun's interests consistent with the terms contained in this Agreement, and (vi) you agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software.

C. License to Distribute Redistributables. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software README file, including but not limited to the Java Technology Restrictions of these Supplemental Terms, Sun grants you a non-exclusive, non-transferable, limited license without fees to reproduce and distribute those files specifically identified as redistributable in the software "README" file ("Redistributables") provided that: (i) you distribute the Redistributables complete and unmodified, and only bundled as part of Programs, (ii) the Programs add significant and primary functionality to the Redistributables, (iii) you do not distribute additional software intended to supersede any component(s) of the Redistributables (unless otherwise specified in the applicable README file), (iv) you do not remove or alter any proprietary legends or notices contained in or on the Redistributables, (v) you only distribute the Redistributables pursuant to a license agreement that protects Sun's interests consistent with the terms contained in the Agreement, (vi) you agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Software.

D. Java Technology Restrictions. You may not create, modify, or change the behavior of, or authorize your licensees to create, modify, or change the behavior of, classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun" or similar convention as specified by Sun in any naming convention designation.

E. Distribution by Publishers. This section pertains to your distribution of the Software with your printed book or magazine (as those terms are commonly used in the industry) relating to Java technology ("Publication"). Subject to and conditioned upon your compliance with the restrictions and obligations contained in the Agreement, in addition to the license granted in Paragraph 1 above, Sun hereby grants to you a non-exclusive, nontransferable limited right to reproduce complete and unmodified copies of the Software on electronic media (the "Media") for the sole purpose of inclusion and distribution with your Publication(s), subject to the following terms: (i) You may not distribute the Software on a stand-alone basis; it must be distributed with your Publication(s); (ii) You are responsible for downloading the Software from the applicable Sun web site; (iii) You must refer to the Software as JavaTM SE Development Kit 6; (iv) The Software must be reproduced in its entirety and without any modification whatsoever (including, without limitation, the Binary Code License and Supplemental License Terms accompanying the Software and proprietary rights notices contained in the Software); (v) The Media label shall include the following information: Copyright 2006, Sun Microsystems, Inc. All rights reserved. Use is subject to license terms. Sun, Sun Microsystems, the Sun logo, Solaris, Java, the Java Coffee Cup logo, J2SE, and all trademarks and logos based on Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. This information must be placed on the Media label in such a manner as to only apply to the Sun Software; (vi) You must clearly identify the Software as Sun's product on the Media holder or Media label, and you may not state or imply that Sun is responsible for any third-party software contained on the Media; (vii) You may not include any third party software on the Media which is intended to be a replacement or substitute for the Software; (viii) You shall indemnify Sun for all damages arising from your failure to comply with the requirements of this Agreement. In addition, you shall defend, at your expense, any and all claims brought against Sun by third parties, and shall pay all damages awarded by a court of competent jurisdiction, or such settlement amount negotiated by you, arising out of or in connection with your use, reproduction or distribution of the Software and/or the Publication. Your obligation to provide indemnification under this section shall arise provided that Sun: (a) provides you prompt notice of the claim; (b) gives you sole control of the defense and settlement of the claim; (c) provides you, at your expense, with all available information, assistance and authority to defend; and (d) has not compromised or settled such claim without your prior written consent; and (ix) You shall provide Sun with a written notice for each Publication; such notice shall include the following information: (1) title of Publication, (2) author(s), (3) date of Publication, and (4) ISBN or ISSN numbers. Such notice shall be sent to Sun Microsystems, Inc., 4150 Network Circle, M/S USCA12-110, Santa Clara, California 95054, U.S.A , Attention: Contracts Administration.

F. Source Code. Software may contain source code that, unless expressly licensed for other purposes, is provided solely for reference purposes pursuant to the terms of this Agreement. Source code may not be redistributed unless expressly provided for in this Agreement.

G. Third Party Code. Additional copyright notices and license terms applicable to portions of the Software are set forth in the THIRDPARTYLICENSEREADME.txt file. In addition to any terms and conditions of any third party opensource/freeware license identified in the THIRDPARTYLICENSEREADME.txt file, the disclaimer of warranty and limitation of liability provisions in paragraphs 5 and 6 of the Binary Code License Agreement shall apply to all Software in this distribution.

H. Termination for Infringement. Either party may terminate this Agreement immediately should any Software become, or in either party's opinion be likely to become, the subject of a claim of infringement of any intellectual property right.

I. Installation and Auto-Update. The Software's installation and auto-update processes transmit a limited amount of data to Sun (or its service provider) about those specific processes to help Sun understand and optimize them. Sun does not associate the data with personally identifiable information. You can find more information about the data Sun collects at http://java.com/data/.

For inquiries please contact: Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A.

PCRE 6.3

Portions of this product include software developed by Philip Hazel. The University of Cambridge Computing Service software is distributed in accordance with the following license agreement.

FONCTIONS DE BIBLIOTHEQUE DE BASE

Auteur : Philip Hazel

Partie locale de messagerie : ph10

Domaine de messagerie : cam.ac.uk

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

Copyright (c) 1997-2006 University of Cambridge

Tous droits réservés.

FONCTIONS WRAPPER EN C++

Contribution : Google Inc.

Copyright (c) 2006, Google Inc.

Tous droits réservés.

LICENCE BSD

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the University of Cambridge nor the name of Google Inc. nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

Zlib 1.2.3

This product includes zlib developed by Jean-loup Gailly and Mark Adler.

/* zlib.h -- interface of the 'zlib' general purpose compression library version 1.2.1, November 17th, 2003

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

*/

ZThread 2.3.2

Certaines parties de ce produit comprennent des logiciels développés par Eric Crahen. Le logiciel ZThread est distribué conformément au contrat de licence suivant.